PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-069548
(43)Date of publication of application : 07.03.2003

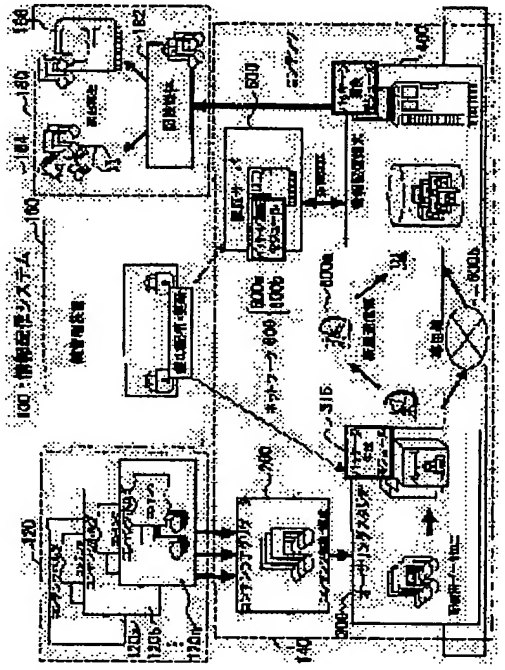
(51)Int.Cl. H04L 9/08
G06F 15/00
G10K 15/02

(21)Application number : 2001-251689
(22)Date of filing : 22.08.2001

(71)Applicant : SONY CORP
(72)Inventor : YOSHITOMI KAZUNORI
YOSHINO KENJI
UENO SHINICHI

(54) AUTHORING SYSTEM, AUTHORING KEY GENERATION DEVICE, AUTHORING DEVICE, AUTHORING METHOD, COMPUTER PROGRAM, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information distribution system capable of preventing unauthorized copying.
SOLUTION: The invention is an authoring system that conducts authoring by encryption for copyright protection for content data distributed via an information distribution terminal 400. An authoring key generating device 160 generates a content identifier (CID) uniquely allocated to each content data, an authoring key usage key (CEK) uniquely allocated to each authoring device that conducts authoring for content data, a content key (Kc) used in encryption of content data, and an authoring key (CED) obtained from encryption of a second content key (EKc) using CID and CEK. The second content key (EKc) is derived from encryption of the content key by a root key (Kroot). An authoring device 316 is provided with a decrypting means for decrypting CED to get Kc and Ekc using CID and CEK, and an encryption means for encrypting content data using the decrypted Kc to generate an authored and encrypted content data (E (Kc, Content)).



LEGAL STATUS

[Date of request for examination] 20.02.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－69548
（P2003－69548A）
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　15/00	３３０Ｚ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｇ１０Ｋ　15/02		５Ｊ１０４
Ｇ１０Ｋ　15/02		Ｈ０４Ｌ　9/00	６０１Ｄ	
			６０１Ｅ	

審査請求　未請求　請求項の数30　ＯＬ　（全 28 頁）

(21)出願番号　特願2001－251689(P2001－251689)

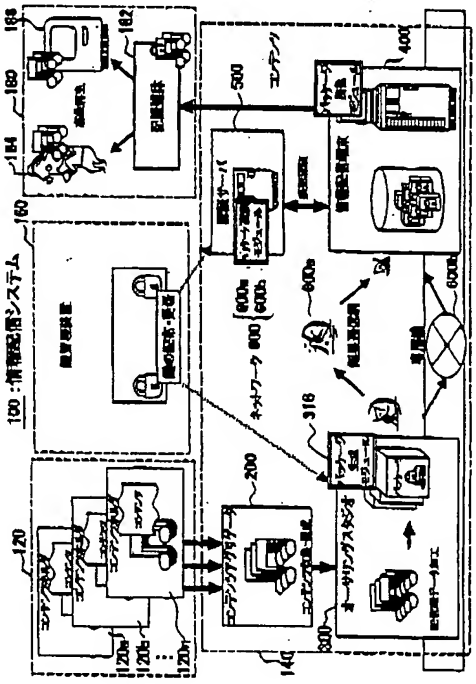
(22)出願日　平成13年８月22日(2001.8.22)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　吉富　和憲
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　吉野　賢治
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100095957
弁理士　亀谷　美明　（外３名）

最終頁に続く

(54)【発明の名称】　オーサリングシステム，オーサリング鍵生成装置，オーサリング装置，オーサリング方法，コンピュータプログラムおよび記憶媒体

(57)【要約】
【課題】　不正コピーを防止可能な情報配信システムを提供する。
【解決手段】　情報配信端末４００を介して配信するコンテンツデータに著作権保護の暗号化を施してオーサリングするオーサリングシステムである。オーサリング鍵生成装置１６０は，コンテンツデータ毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，コンテンツデータをオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，コンテンツデータを暗号化するコンテンツ鍵（Ｋｃ）およびコンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）をＣＩＤおよびＣＥＫを用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成する。オーサリング装置３１６は，ＣＥＤから，ＣＩＤとＣＥＫを用いてＫｃとＥＫｃとを復号化する復号化手段と，復号化したＫｃを用いてコンテンツデータを暗号化し，オーサリングされた暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化手段と備えている。



1

【特許請求の範囲】

【請求項１】 情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするオーサリングシステムであって：前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，コンテンツデータ（Ｃｏｎｔｅｎｔ）をオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成するオーサリング鍵生成装置と；前記オーサリング鍵（ＣＥＤ）から，前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）を用いて，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）とを復号化する復号化手段と，復号化した前記コンテンツ鍵（Ｋｃ）を用いて前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化し，オーサリングされた暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化手段と備えたオーサリング装置と；から成ることを特徴とする，オーサリングシステム。

【請求項２】 前記オーサリング装置は，前記暗号化手段によって得られる暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））と，前記コンテンツ識別子（ＣＩＤ）と，前記第２のコンテンツ鍵（ＥＫｃ）とを一つのパッケージデータとしてパッケージ化するパッケージ手段をさらに備えることを特徴とする，請求項１に記載のオーサリングシステム。

【請求項３】 前記コンテンツ鍵（Ｋｃ）は，前記第２のコンテンツ鍵（ＥＫｃ）と前記ルート鍵（Ｋｒｏｏｔ）から得られる鍵であって，前記暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を復号可能とし，前記ルート鍵（Ｋｒｏｏｔ）をセキュアに保持する再生装置において前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を再生可能とすることを特徴とする，請求項１に記載のオーサリングシステム。

【請求項４】 前記ルート鍵（Ｋｒｏｏｔ）は，前記再生装置に関連するデバイス鍵（Ｋｄｅｖｉｃｅ）により暗号化されたコンテンツ使用可能化鍵（ＥＫＢ）に組み込まれて保持されており，前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えて前記コンテンツ使用可能化鍵（ＥＫＢ）も暗号化されていることを特徴とする，請求項３に記載のオーサリングシステム。

【請求項５】 前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（Ｅ

2

Ｋｃ）に加えてチェックサム情報も暗号化されていることを特徴とする，請求項１に記載のオーサリングシステム。

【請求項６】 前記オーサリング鍵（ＣＥＫ）の更新があった場合には，更新前のオーサリング鍵（ＣＥＫ）の破棄を行う破棄手段をさらに備えることを特徴とする，請求項１に記載のオーサリングシステム。

【請求項７】 前記コンテンツデータ（Ｃｏｎｔｅｎｔ）は，メインコンテンツデータとメインコンテンツデータの付加情報とから成ることを特徴とする，請求項１に記載のオーサリングシステム。

【請求項８】 情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするためのオーサリング鍵を生成するオーサリング鍵生成装置であって：前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）をオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成することを特徴とする，オーサリング鍵生成装置。

【請求項９】 前記コンテンツ鍵（Ｋｃ）は，前記第２のコンテンツ鍵（ＥＫｃ）と前記ルート鍵（Ｋｒｏｏｔ）から得られる鍵であって，前記暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を復号可能とし，前記ルート鍵（Ｋｒｏｏｔ）をセキュアに保持する再生装置において前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を再生可能とすることを特徴とする，請求項８に記載のオーサリング鍵生成装置。

【請求項１０】 前記ルート鍵（Ｋｒｏｏｔ）は，前記再生装置に関連するデバイス鍵（Ｋｄｅｖｉｃｅ）により暗号化されたコンテンツ使用可能化鍵（ＥＫＢ）に組み込まれて保持されており，前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えて前記コンテンツ使用可能化鍵（ＥＫＢ）も暗号化されていることを特徴とする，請求項８に記載のオーサリング鍵生成装置。

【請求項１１】 前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えてチェックサム情報も暗号化されていることを特徴とする，請求項８に記載のオーサリング鍵生成装置。

【請求項１２】 前記オーサリング鍵（ＣＥＫ）の更新があった場合には，更新前のオーサリング鍵（ＣＥＫ）の破棄を行う破棄手段をさらに備えることを特徴とす

る，請求項８に記載のオーサリング鍵生成装置。

【請求項１３】 情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするためのオーサリング鍵を生成するオーサリング鍵生成装置であって：コンピュータを，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）をオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成するオーサリング鍵生成装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項１４】 情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするためのオーサリング鍵を生成するオーサリング鍵生成装置であって：コンピュータを，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）をオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成するオーサリング鍵生成装置として機能させるコンピュータプログラムが格納されたコンピュータ読み取り可能な記憶媒体。

【請求項１５】 情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするオーサリング装置において：前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を記憶するコンテンツ記憶手段と；前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，前記オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）と，から成る鍵情報を記憶する鍵情報記憶手段と；前記オーサリング鍵（ＣＥＤ）から，前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）を用いて，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）とを復号化する復号化手段と前記コンテンツ鍵（Ｋｃ）を用いて前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化して暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化手段と，を備えることを特徴とする，オーサリング装置

【請求項１６】 さらに，前記暗号化手段によって得られる暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））と，前記コンテンツ識別子（ＣＩＤ）と，前記第２のコンテンツ鍵（ＥＫｃ）とを一つのパッケージデータとしてパッケージ化するパッケージ手段と：を備えることを特徴とする，請求項１５に記載のオーサリング装置。

【請求項１７】 前記オーサリング鍵（ＣＥＤ）は，前記パッケージデータ作成装置とは別体に構成された権限のあるオーサリング鍵生成装置において暗号化されることを特徴とする，請求項１５に記載のオーサリング装置。

【請求項１８】 前記コンテンツ鍵（Ｋｃ）は，前記第２のコンテンツ鍵（ＥＫｃ）と前記ルート鍵（Ｋｒｏｏｔ）から得られる鍵であって，前記暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を復号可能とし，前記ルート鍵（Ｋｒｏｏｔ）をセキュアに保持する再生装置において前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を再生可能とすることを特徴とする，請求項１５に記載のオーサリング装置。

【請求項１９】 前記ルート鍵（Ｋｒｏｏｔ）は，前記再生装置に関連するデバイス鍵（Ｋｄｅｖｉｃｅ）により暗号化されたコンテンツ使用可能化鍵（ＥＫＢ）として保持されており，前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えて前記コンテンツ使用可能化鍵（ＥＫＢ）も暗号化されていることを特徴とする，請求項１８に記載のオーサリング装置。

【請求項２０】 前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えてチェックサム情報も暗号化されていることを特徴とする，請求項１５に記載のオーサリング装置。

【請求項２１】 前記オーサリング鍵（ＣＥＫ）の更新があった場合には，更新前のオーサリング鍵（ＣＥＫ）の破棄を行う破棄手段をさらに備えることを特徴とする，請求項１５に記載のオーサリング装置。

【請求項２２】 前記コンテンツデータ（Ｃｏｎｔｅｎｔ）は，メインコンテンツデータとメインコンテンツデータの付加情報とから成ることを特徴とする，請求項１５に記載のオーサリング装置。

【請求項２３】 前記パッケージ手段は，さらに前記コ

ンテンツデータ（Ｃｏｎｔｅｎｔ）に関する付加情報であるフリンジデータを合わせてパッケージ化することを特徴とする，請求項１５に記載のオーサリング装置。

【請求項２４】　情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするオーサリング装置において：コンピュータを，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を記憶するコンテンツ記憶手段と；前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，前記オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）と，から成る鍵情報を記憶する鍵情報記憶手段と；前記オーサリング鍵（ＣＥＤ）から，前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）を用いて，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）とを復号化する復号化手段と前記コンテンツ鍵（Ｋｃ）を用いて前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化して暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化手段と，して機能せしめることを特徴とするコンピュータプログラム。

【請求項２５】　情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするオーサリング装置において：コンピュータを，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を記憶するコンテンツ記憶手段と；前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，前記オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）と，から成る鍵情報を記憶する鍵情報記憶手段と；前記オーサリング鍵（ＣＥＤ）から，前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）を用いて，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）とを復号化する復号化手段と前記コンテンツ鍵（Ｋｃ）を用いて前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化して暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化手段と，して機能させるコンピュータプログラムを記録したコンピュータ読み取り可能な記憶媒体。

【請求項２６】　情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするオーサリング方法であって：前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成するオーサリング鍵生成段階と；前記オーサリング鍵（ＣＥＤ）から，前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）を用いて，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）とを復号化する復号化段階と；復号化した前記コンテンツ鍵（Ｋｃ）を用いて前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化し，オーサリングされた暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化段階と；から成ることを特徴とする，オーサリング方法。

【請求項２７】　さらに，前記暗号化装置によって得られる暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））と，前記コンテンツ識別子（ＣＩＤ）と，前記第２のコンテンツ鍵（ＥＫｃ）とを一つのパッケージデータとしてパッケージ化するパッケージ段階を含むことを特徴とする，請求項２６に記載のオーサリング方法。

【請求項２８】　前記ルート鍵（Ｋｒｏｏｔ）は，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を生成可能な再生装置に関連するデバイス鍵（Ｋｄｅｖｉｃｅ）により暗号化されたコンテンツ使用可能化鍵（ＥＫＢ）に組み込まれて保持されており，前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えて前記コンテンツ使用可能化鍵（ＥＫＢ）も暗号化されていることを特徴とする，請求項２６に記載のオーサリング方法。

【請求項２９】　前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えてチェックサム情報も暗号化されていることを特徴とする，請求項２６に記載のオーサリング方法。

【請求項３０】　前記オーサリング鍵（ＣＥＫ）の更新があった場合には，更新前のオーサリング鍵（ＣＥＫ）の破棄を行う破棄段階をさらに含むことを特徴とする，請求項２６に記載のオーサリング方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，セキュアに楽曲などのコンテンツを配信する情報配信システムに係り，特

にメモリスティックなどの記憶媒体にコンテンツをセキュアにダウンロードすることが可能な情報提供装置，情報配信端末，情報提供方法，コンピュータプログラムおよび記憶媒体を介して配信するコンテンツデータに対して，著作権保護の暗号化を施してオーサリングするオーサリングシステム，オーサリング用の鍵を生成するオーサリング鍵生成装置，コンテンツを暗号化してオーサリングするオーサリング装置，オーサリング方法，コンピュータプログラムおよび記憶媒体に関する。

【０００２】

【従来の技術】近年，インターネットなどのネットワークの普及とともに，音楽データ，画像（静止画および動画を含む）データ，ゲームプログラムなどの様々な情報（以下，コンテンツという。）をネットワークを介してユーザに対して配信する情報配信システムの構築が提案されている。かかる情報配信システムの構築には，各コンテンツに付随する著作権の保護をどのように担保するかが重要な前提となる。すなわち，ネットワークを介することで，各コンテンツの大量のデジタルコピーが可能となってしまう。そのため，コンテンツの違法コピーを防ぐためのいくつかの著作権保護技術が開発されている。

【０００３】

【発明が解決しようとする課題】一般に，配信されるコンテンツを違法コピーから保護するためには，二つの暗号化段階が必要であると言われている。第一の暗号化段階は，コンテンツをオーサリングする際に，コンテンツを暗号化し，コンテンツ配信時の違法コピーを保護する段階である。第二の暗号化段階は，キオスク端末などの情報配信端末を介して，ユーザが所有する記憶装置にコンテンツを書き出す際に，コンテンツを暗号化し，その後の違法コピーを防止する段階である。

【０００４】この点，従来のコンテンツ配信サービスにおいては，オーサリング時の暗号化方式と，書き出し時の暗号方式が異なっていた。このため，ユーザが所有する記憶装置にコンテンツを書き出す際に，一旦コンテンツの復号化を行い，再び暗号化するというステップを踏まなければならず，処理に余計な時間を要していた。また，書き出し時の復号化の際に，一時的にコンテンツが生の状態になってしまうためセキュリティ上も問題があった。

【０００５】また，従来の情報配信システムにおいては，コンテンツの書き込みモジュールに，使用許可認証機能が備わっていなかったため，書き込みモジュール自体の盗難に対しては無防備であった。すなわち，盗難された書き込みモジュールにより，コンテンツの大量のデジタルコピーを不正に行うことが可能となってしまうという問題もあった。

【０００６】さらにまた，従来の情報配信システムにおいては，オーサリング処理自体のプロテクトが甘く，オーサリングの仕様書を入手すれば，誰でもコンテンツのオーサリングが可能となってしまうという問題もあった。

【０００７】さらにまた，従来の情報配信システムにおいては，例えばコンテンツが音楽データの場合には，ユーザが一旦コンテンツをユーザ所有の記憶装置にダウンロードした後に，他のメディアにコンテンツを移動させたい場合に，正規にコンテンツを入手した正規ユーザであっても，音質を劣化させずに，自由にコンテンツを移動させることはできないという問題もあった。

【０００８】さらにまた，従来の情報配信システムにおいては，例えばコンテンツが音楽データである場合には，楽曲とタイトルしかMDなどのメディアに記録できず，ジャケット写真や歌詞データ等の付随データ（いわゆる，フリンジデータ）については，プリンタによりプリントアウトするなどして入手しなければならないという問題もあった。

【０００９】本発明は，従来の情報配信システムが有する上記および以下に言及されるような各種問題点を解決することを目的としている。

【００１０】

【課題を解決するための手段】上記課題を解決するために，本発明のある観点によれば，情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするオーサリングシステムが提供される。このオーサリングシステムは，オーサリング鍵生成装置とオーサリング装置とから構成されている。

【００１１】オーサリング鍵生成装置は，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成する。

【００１２】オーサリング装置は，前記オーサリング鍵（ＣＥＤ）から，前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）を用いて，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）とを復号化する復号化手段と，復号化した前記コンテンツ鍵（Ｋｃ）を用いて前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化し，オーサリングされた暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化手段とを備えている。

【００１３】オーサリング装置は，前記暗号化手段によって得られる暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））と，前記コンテンツ識別子（ＣＩＤ）

と，前記第２のコンテンツ鍵（ＥＫｃ）とを一つのパッケージデータとしてパッケージ化するパッケージ手段をさらに備えてもよい。

【００１４】上記課題を解決するために本発明の別の観点によれば，情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするためのオーサリング鍵を生成するオーサリング鍵生成装置であって：前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成することを特徴とする，オーサリング鍵生成装置が提供される。

【００１５】さらに本発明の別の観点によれば，情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするオーサリング装置において：前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を記憶するコンテンツ記憶手段と；前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，前記オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテンツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）と，から成る鍵情報を記憶する鍵情報記憶手段と；前記オーサリング鍵（ＣＥＤ）から，前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）を用いて，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）とを復号化する復号化手段と；前記コンテンツ鍵（Ｋｃ）を用いて前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化して暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化手段とを備えることを特徴とする，オーサリング装置が提供される。

【００１６】このオーサリング装置は，さらに，前記暗号化手段によって得られる暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））と，前記コンテンツ識別子（ＣＩＤ）と，前記第２のコンテンツ鍵（ＥＫｃ）とを一つのパッケージデータとしてパッケージ化するパッケージ手段を備えてもよい。

【００１７】また，前記オーサリング鍵（ＣＥＤ）は，前記パッケージデータ作成装置とは別体に構成された権限のあるオーサリング鍵生成装置において暗号化されるように構成してもよい。

【００１８】さらに，前記パッケージ手段は，さらに前記コンテンツデータ（Ｃｏｎｔｅｎｔ）に関する付加情報であるプリンジデータを合わせてパッケージ化するように構成してもよい。

【００１９】さらに本発明の別の観点によれば，コンピュータをして上記オーサリング鍵生成装置または上記オーサリング装置として機能せしめることを特徴とするコンピュータプログラムおよびそのコンピュータプログラムが格納されたコンピュータ読み取り可能な記憶媒体が提供される。

【００２０】上記オーサリングシステム，オーサリング鍵生成装置，オーサリング装置において，前記コンテンツ鍵（Ｋｃ）は，前記第２のコンテンツ鍵（ＥＫｃ）と前記ルート鍵（Ｋｒｏｏｔ）から得られる鍵であって，前記暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を復号可能とし，前記ルート鍵（Ｋｒｏｏｔ）をセキュアに保持する再生装置において前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を再生可能とするように構成してもよい。

【００２１】前記ルート鍵（Ｋｒｏｏｔ）は，前記再生装置に関連するデバイス鍵（Ｋｄｅｖｉｃｅ）により暗号化されたコンテンツ使用可能化鍵（ＥＫＢ）に組み込まれて保持されており，前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えて前記コンテンツ使用可能化鍵（ＥＫＢ）も暗号化されているように構成してもよい。

【００２２】また，前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えてチェックサム情報も暗号化するように構成してもよい。

【００２３】さらに，前記オーサリング鍵（ＣＥＫ）の更新があった場合には，更新前のオーサリング鍵（ＣＥＫ）の破棄を行う破棄手段をさらに備えるように構成してもよい。

【００２４】本情報配布システムの情報配布対象である前記コンテンツデータ（Ｃｏｎｔｅｎｔ）は，メインコンテンツデータとメインコンテンツデータの付加情報とを含んでいる。

【００２５】さらに本発明の別の観点によれば，情報配信端末を介して配信するコンテンツデータ（Ｃｏｎｔｅｎｔ）に対して著作権保護の暗号化を施してオーサリングするオーサリング方法であって：前記コンテンツデータ（Ｃｏｎｔｅｎｔ）毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）と，オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）と，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化するコンテンツ鍵（Ｋｃ）および前記コンテンツ鍵をルート鍵（Ｋｒｏｏｔ）で暗号化した第２のコンテン

ツ鍵（ＥＫｃ）を前記コンテンツ識別子（ＣＩＤ）および前記オーサリング鍵使用鍵（ＣＥＫ）を用いて暗号化したオーサリング鍵（ＣＥＤ）とを生成するオーサリング鍵生成段階と；前記オーサリング鍵（ＣＥＤ）から，前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）を用いて，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）とを復号化する復号化段階と；復号化した前記コンテンツ鍵（Ｋｃ）を用いて前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を暗号化し，オーサリングされた暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する暗号化段階と；から成ることを特徴とする，オーサリング方法が提供される。

【００２６】上記オーサリング方法は，さらに，前記暗号化装置によって得られる暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））と，前記コンテンツ識別子（ＣＩＤ）と，前記第２のコンテンツ鍵（ＥＫｃ）とを一つのパッケージデータとしてパッケージ化するパッケージ段階を含んでもよい。

【００２７】前記ルート鍵（Ｋｒｏｏｔ）は，前記コンテンツデータ（Ｃｏｎｔｅｎｔ）を生成可能な再生装置に関連するデバイス鍵（Ｋｄｅｖｉｃｅ）により暗号化されたコンテンツ使用可能化鍵（ＥＫＢ）に組み込まれて保持されており，前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えて前記コンテンツ使用可能化鍵（ＥＫＢ）も暗号化されているように構成しても良い。

【００２８】前記オーサリング鍵（ＣＥＫ）には，前記コンテンツ鍵（Ｋｃ）と前記第２のコンテンツ鍵（ＥＫｃ）に加えてチェックサム情報も暗号化されているように構成してもよい。

【００２９】前記オーサリング鍵（ＣＥＫ）の更新があった場合には，更新前のオーサリング鍵（ＣＥＫ）の破棄を行う破棄段階をさらに含むように構成しても良い。

【００３０】本発明のさらに別の目的，特徴，作用効果については，以下に述べる発明の実施形態および添付図面により明らかになろう。

【００３１】

【発明の実施形態】以下に添付図面を参照しながら，本発明にかかる情報配信システム等の好適な実施形態として，当該システムを音楽データをコンテンツとして配信する情報配信システムに適用した場合について説明する。なお，以下の説明および添付図面において，略同一の機能構成を有する部材については，同一の符号を付することにより重複説明を省略することにする。

【００３２】（１．　配信対象となる情報）まず，本実施の形態にかかる情報配信システムの理解を容易にするために，情報配信システムの配信対象となる情報について説明する。

【００３３】本実施の形態にかかる情報配信システムにおける配信対象となる情報は，「配信用コンテンツ」である。配信用コンテンツは，メインコンテンツと付加情報を含んでいる。なお，本明細書において，単に「コンテンツ（データ）」と称した場合には，後述するメインコンテンツと付加情報の双方を含むものとする。

【００３４】「メインコンテンツ（データ）（Ｍａｉｎ　Ｃｏｎｔｅｎｔ　Ｄａｔａ）」は，本実施の形態にかかる情報配信システムにおける主たる配信対象となる情報である。より具体的には，コンテンツホルダにより制作される楽曲データ，画像データ（静止画像データおよび動画像データを含む），ゲームプログラムなどである。

【００３５】「付加情報」は，メインコンテンツに付随するデータである。例えば，メインデータが楽曲データである場合には，それに付随したジャケット写真や歌詞などといったフリンジデータ（Ｆｒｉｎｇｅ　Ｄａｔａ）や，楽曲のタイトルやアーティスト名などのメタデータ（Ｍｅｔａｄａｔａ）や，他の装置へのチェックアウト（Ｃｈｅｃｋ　Ｏｕｔ）可能回数やコンピュータ装置への移動（Ｉｍｐｏｒｔ）可能回数などの利用条件情報などを含んでいる。

【００３６】「パッケージ（データ）（パッケージ情報（Ｐａｃｋａｇｅ　Ｄａｔａ））」は，本実施の形態にかかる情報配信システムにおいて，情報配信端末から配信する配信用コンテンツデータに対して，著作権保護の暗号化を施してパッケージ化したものである。パッケージデータは，オーサリングスタジオ３００のパッケージ情報生成部３１６により生成される。パッケージには，メインコンテンツおよび付加情報を暗号化した暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））に加えて，後述する第２のコンテンツ鍵（ＥＫｃ）およびコンテンツ使用可能化鍵（ＥＫＢ）なども含まれている。

【００３７】（２．　情報配信システムの概要）図１に，本実施の形態にかかる情報配信システム１００の概略構成を示す。図１に示すように，情報配信システム１００は，コンテンツホルダ部１２０と，コンテンツ流通部１４０と，鍵管理装置１６０と，ユーザ部１８０とから主に構成されている。以下，各構成要素について説明する。

【００３８】（２．１　コンテンツホルダ（Ｃｏｎｔｅｎｔ　Ｈｏｌｄｅｒ）部１２０）コンテンツホルダ部１２０は，レコード会社に所属するサーバのような情報処理装置群である。コンテンツホルダ部は同様の機能を有する複数のコンテンツホルダ１２０ａ～１２０ｎから構成されている。各コンテンツホルダ１２０ａ～１２０ｎは，例えば，図２に示すように，コンテンツ管理部１２２と，コンテンツ作成部１２４と，コンテンツ出力部１２６と，コンテンツデータベース１２８とを備えたコンピュータなどのサーバ装置である。

【００３９】（コンテンツ管理部１２２）コンテンツ管

理部１２２は，当該コンテンツホルダ１２０ａに関連するレコード会社などにより制作された楽曲データなどのコンテンツを管理する。ここで管理されるコンテンツには，コンテンツが音楽関連情報の場合には，楽曲データなどのメインコンテンツに加え，ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【００４０】（コンテンツ作成部１２４）コンテンツ作成部１２４は，当該コンテンツホルダ１２０ａに関連するコンテンツを作成する。ここで作成されるコンテンツには，コンテンツが音楽関連情報の場合には，楽曲データなどのメインコンテンツに加え，ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【００４１】（コンテンツ出力部１２６）コンテンツ出力部１２６は，当該コンテンツホルダ１２０ａにおいて作成管理されるコンテンツを，後述するようなコンテンツ流通部１４０のコンテンツアグリゲータ２００に受け渡す。コンテンツの受け渡しは，インターネットなどのネットワークを介して行ってもよいし，あるいは，ＣＤ－ＲやＤＶＤ－ＲＡＭなどの記憶メディアを介して行ってもよい。

【００４２】（コンテンツデータベース１２８）コンテンツデータベース１２８は，コンテンツ作成部１２４により作成されたコンテンツを記憶する大容量記憶メディアである。ここで記憶され管理されるコンテンツには，コンテンツが音楽関連情報の場合には，楽曲データなどのメインコンテンツに加え，ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【００４３】（２．２　コンテンツ流通部）コンテンツ流通部１４０は，本実施の形態にかかる情報配信システムの中核をなす部分である。このコンテンツ流通部１４０において，配信用コンテンツに対して著作権保護のための暗号化が施され，パッケージデータとしてパッケージ化される。パッケージ化されたパッケージデータは，ネットワーク６００を介してキオスク端末などの情報配信端末４００に送られ，情報配信端末４００からユーザが所有する記憶装置１８２に提供される。

【００４４】コンテンツ流通部１４０は，コンテンツアグリゲータ部２００と，オーサリングスタジオ部３００と，情報配信部（キオスク端末部）４００と，認証サーバ部５００と，ネットワーク６００とから主に構成されている。

【００４５】（２．２．１　コンテンツアグリゲータ（Ｃｏｎｔｅｎｔ　Ａｇｇｒｅｇａｔｅｒ）２００）コンテンツアグリゲータ２００は，コンテンツホルダ１２０から楽曲などのコンテンツを収集し，企画編成する業務を行う。ここで収集されるコンテンツには，コンテンツが音楽関連情報の場合には，楽曲データなどのメインコンテンツに加え，ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【００４６】コンテンツアグリゲータ２００は，コンテンツ管理部２１０と，コンテンツ収集部２２０と，コンテンツ出力部２３０と，コンテンツデータベース２４０とから主に構成されている。

【００４７】（コンテンツ管理部２１０）コンテンツ管理部２１０は，コンテンツホルダ１２０ａ～１２０ｎが保持しているコンテンツの中から，情報配信システム１００を利用して配信を行う魅力と価値のあるコンテンツを選択する。さらにコンテンツ管理部２１０は，コンテンツ収集部２２０に対して，所定のコンテンツホルダ１２０ａに直接アクセスして，あるいは所定のコンテンツホルダ１２０ａから配布されるメディアにアクセスして，コンテンツを収集するように指令を行う。コンテンツ管理部２１０は，コンテンツホルダ１２０から収集したコンテンツの企画編成も同時に行う。

【００４８】（コンテンツ収集部２２０）コンテンツ収集部２２０は，コンテンツ管理部２１０からの指令を受けて，所定のコンテンツホルダ１２０ａに直接アクセスして，あるいは所定のコンテンツホルダ１２０ａから配布されるメディアにアクセスして，コンテンツを取り込み，コンテンツデータベース２４０に記憶する。

【００４９】（コンテンツデータベース２４０）コンテンツデータベース２４０は，コンテンツ収集部２２０が取り込んだコンテンツを一時的に記憶して管理する。またコンテンツデータベース２４０は，コンテンツアグリゲータ２００の動作に関する各種履歴を記憶して管理する。

【００５０】（コンテンツ出力部２３０）コンテンツ出力部２３０は，後述するオーサリングスタジオ３００からの要求に応じて，コンテンツ収集部２２０が収集したコンテンツをコンテンツデータベース２４０から読み出し，オーサリングスタジオ３００に対して出力する。オーサリングスタジオ３００へのコンテンツの出力は，インターネットなどの公衆回線網を介して行ってもよいし，よりセキュアな専用回線網を介しておこなってもよい。さらには，ＣＤ－ＲやＤＶＤ－ＲＡＭなどの記憶媒体を介して行ってもよい。

【００５１】（２．２．２　オーサリングスタジオ３００）オーサリングスタジオ３００は，配布対象であるコンテンツを本実施の形態にかかる情報配信システムに適合するように加工する機能を有する。より具体的に言えば，コンテンツデータの加工は，コンテンツを配布しやすいように圧縮する第一段階と，オーサリングして暗号

化し，さらにパッケージ化する第二段階を経て行われる。

【００５２】図４に示すように，オーサリングスタジオ３００は，オーサリング部３１０と商品管理部３３０とデータベースサーバ３４０とから主に構成されている。

【００５３】（オーサリング部３１０）オーサリング部３１０は，例えばコンピュータ装置上で動作するコンピュータプログラムであり，図５に示すように，コンテンツ管理部３１２と，データ圧縮部３１４と，パッケージ生成モジュール３１６と，ＧＵＩ制作部３１８と，配信部３２０とを備えている。

【００５４】（コンテンツ管理部３１２）コンテンツ管理部３１２は，コンテンツアグリゲータ２００から受信したコンテンツを管理する。ここで管理されるコンテンツには，コンテンツが音楽関連情報の場合には，楽曲データなどのメインコンテンツに加え，ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【００５５】（データ圧縮部３１２）データ圧縮部３１２は，例えば，コンテンツ管理部３１２から受け渡されたコンテンツを圧縮加工するソフトウェアである。圧縮方式としては，例えばコンテンツが楽曲データであるような場合には，ＡＴＲＡＣ３方式を採用して，元データを約１／１０に圧縮加工することが可能である。もちろん，圧縮方式は，ＡＴＲＡＣ３（Ａｄａｐｔｉｖｅ Ｔｒａｎｓｆｏｒｍ Ａｃｏｕｓｔｉｃ Ｃｏｄｉｎｇ ３）に限定されず，ＭＰ３（ＭＰＥＧ－１ Ａｕｄｉｏ Ｌａｙｅｒ３）方式，ＡＡＣ（Ａｄｖａｎｃｅｄ Ａｕｄｉｏ Ｃｏｄｉｎｇ）方式，ＷＭＡ（Ｗｉｎｄｏｗｓ（登録商標） Ｍｅｄｉａ Ａｕｄｉｏ）方式，Ｔｗｉｎ ＶＱ（Ｔｒａｎｓｆｏｒｍ－Ｄｏｍａｉｎ Ｗｅｉｇｈｔｅｄ Ｉｎｔｅｒｌｅａｖｅ Ｖｅｃｔｏｒ Ｑｕａｎｔｉｚａｔｉｏｎ）方式，ＱＤＸ方式などの音声圧縮方式を採用することが可能であることはいうまでもない。

【００５６】（パッケージ生成部（オーサリング装置）３１６）パッケージ生成部（オーサリング装置）３１６は，例えば，データ圧縮部３１４において圧縮加工されたコンテンツデータをオーサリングするために暗号化するとともにパッケージ化する機能を有するソフトウェアとして構成される。すなわち，パッケージ生成部３１６は，コンテンツデータをオーサリングするオーサリング装置として機能する。

【００５７】オーサリング装置３１６の構成およびオーサリング装置で用いられるいくつかの鍵の詳細については，オーサリング鍵生成装置１６０と関連して後述することとし，ここでは簡単な説明にとどめる。

【００５８】オーサリング装置３１６は，図６に示すように，コンテンツ鍵（Ｋｃ）復号化手段３１６２と，コンテンツ暗号化手段３１６４と，パッケージ手段３１６６とから主に構成されている。

【００５９】（コンテンツ鍵（Ｋｃ）復号化手段３１６２）コンテンツ鍵（Ｋｃ）復号化手段３１６２は，後述するオーサリング鍵生成装置１６０から，オーサリング鍵（ＣＥＤ）と前記コンテンツ識別子（ＣＩＤ）と前記オーサリング鍵使用鍵（ＣＥＫ）とを受け取る。そして，オーサリング鍵（ＣＥＤ）から，コンテンツ識別子（ＣＩＤ）とオーサリング鍵使用鍵（ＣＥＫ）を用いて，コンテンツ鍵（Ｋｃ）と第２のコンテンツ鍵（ＥＫｃ）とを復号化する。

【００６０】（コンテンツ暗号化手段３１６４）コンテンツ暗号化手段３１６４は，コンテンツ鍵（Ｋｃ）復号化手段３１６２により復号化した前記コンテンツ鍵（Ｋｃ）を用いて，コンテンツデータを暗号化し，暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））を生成する。本実施の形態にかかる情報配信システムでは，この暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））が所定の情報とともにパッケージ化されて情報配信端末４００に送信される。

【００６１】（パッケージ手段３１６６）パッケージ手段３１６６は，コンテンツ暗号化手段３１６４によって得られる暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））と，コンテンツ識別子（ＣＩＤ）と，第２のコンテンツ鍵（ＥＫｃ）とを一つのパッケージデータとしてパッケージ化する。パッケージには，楽曲データなどのメインコンテンツに加え，ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報も含まれる。

【００６２】（パッケージ生成部３１６の機能構成図）図７には，パッケージ生成部３１６の機能をより具体的に示すブロック図が示されている。図示のように，パッケージ生成部３１６は，Ｗｉｎｄｏｗｓ２０００のようなＯＳ３１０ａ上で動作するオーサリングアプリケーション３１０ｂとして構成されている。オーサリングアプリケーション３１０ｂ内には，データ圧縮部３１４とパッケージ生成部３１６などがＤＬＬ（Ｄｙｎａｍｉｃ Ｌｉｎｋ Ｌｉｂｒａｒｙ）として，組み込まれている。なお，オーサリングアプリケーション３１０ｂに組み込まれるコンテンツ管理部３１２などの他のアプリケーションは説明の便宜のため図示を省略している。

【００６３】図示のように，所定の音声形式，例えばＷＡＶ形式で構成された圧縮前の楽曲データがデータ圧縮部３１４に送られ，所定の圧縮形式，例えばＡＴＲＡＣ３形式で圧縮される。データ圧縮部３１４において圧縮された楽曲データなどのメインコンテンツは，パッケージ生成部３１６に送られ，フリンジデータやメタデータや利用条件情報などから構成される付加情報とともに，暗号化され，パッケージ化される。

【0064】このように，本実施の形態にかかるオーサリング装置（パッケージ生成装置）３１６によれば，オーサリング時に，データ圧縮，暗号化，パッケージ化といった処理を行ってしまうことが可能である。その結果，コンテンツの流通時やコンテンツの販売時における演算付加や通信負荷を軽減することができる。特に情報配布端末におけるダウンロード時間が大幅に縮小可能であり，ユーザは，コンテンツのコピー時間とほとんど変わらない時間でオーサリングされたコンテンツのダウンロードを行うことができる。

【0065】（ＧＵＩ制作部３１８）　再び図５を参照して，オーサリング部３１０のＧＵＩ制作部３１８は，後述する情報配信端末であるキオスク端末に表示されるＧＵＩ（Ｇｒａｐｈｉｃａｌ　Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）を制作する機能を有する。ここで制作されたＧＵＩは，配信部３２０を介して，各キオスク端末に配布される。コンテンツをダウンロードしたいユーザは，このＧＵＩに基づいてキオスク端末上に表示される画面にナビゲートされながら，コンテンツを購入し，所定の記憶媒体にダウンロードしたり，あるいはダウンロードしたコンテンツをコンピュータ装置などの移動（Ｉｍｐｏｒｔ）したり，そのコンピュータ装置などから他の再生装置や記憶媒体にチェックアウトしたりすることが可能である。

【0066】（配信部３２０）配信部３２０は，上記のようにデータ圧縮部３１４およびパッケージ生成部３１８を含むパッケージアプリケーションにより圧縮され，パッケージ化されたコンテンツや，ＧＵＩ制作部３１８において制作されたＧＵＩを，キオスク端末などの情報配信端末４００に配信する機能を有している。

【0067】（商品管理部３３０）再び図４を参照して，商品管理部３３０は，オーサリング部３１０において，配信用に加工されたコンテンツをパッケージ商品として管理する。具体的には，商品管理部３３０は，パッケージ化されたコンテンツの流通を監視し，キオスク管理センタの販売管理部などと連携して，商品の販売および代金回収業務を行う。また商品管理部３３０は，情報配信端末であるキオスク端末４００における販売履歴などについても統計的に把握して管理し，将来的な商品開発の資料とする。商品管理部３３０の業務履歴は，データベースサーバ３４０に記憶される。

【0068】（データベースサーバ３４０）データベースサーバ３４０は，オーサリングスタジオ３００に関連する各種データを記憶して管理する。具体的には，データベースサーバ３４０は，オーサリング３１０において，配信用に加工されたコンテンツを記憶する。ここで管理されるコンテンツには，コンテンツが音楽関連情報の場合には，楽曲データなどのメインコンテンツに加え，ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【0069】また，データベースサーバ３４０には，商品管理部３３０の業務履歴，すなわち，パッケージ商品の販売情報や代金回収情報，情報配信端末であるキオスク端末における販売履歴などについて記憶して管理する。

【0070】（２．２．３　情報配信端末４００）情報配信端末４００は，キオスク端末とも称されるものであり，オーサリングスタジオ３００から配信されたパッケージ化されたコンテンツを記憶し，ユーザ１８０からの要求に応じて該当するコンテンツをユーザ１８０の記憶媒体１８２にダウンロードする機能を有する。キオスク端末４００は，コンビニエンスストアやガソリンスタンドなどの人が集まりやすい場所に設置しても構わないし，各個人が利用する場所に設置されるパーソナルコンピュータ装置を情報配信端末としても構わない。

【0071】情報配信端末４００は，図８に記載されているように，情報配信端末管理部４１０，情報提供部４２０，リーダ／ライタ（Ｒ／Ｗ）４３０，販売管理部４４０，課金制御部４５０，データベース４６０から主に構成されている。

【0072】（情報配信端末管理部４１０）情報配信端末管理部４１０は，例えば，情報配信端末４００におけるさまざまな業務を管理するソフトウェアである。情報配信端末管理部４１０は，情報提供部４２０およびリーダ／ライタ（Ｒ／Ｗ）４３０と連携して，情報配信端末装置の外部認証および内部認証を管理するとともに，認証終了後には，リーダ／ライタ（Ｒ／Ｗ）４３０を介してメモリスティックなどの記憶装置１８２へのコンテンツの書き込みを許可する。

【0073】情報配信端末管理部４１０は，販売管理部４４０および課金制御部４５０と連携して，ユーザ部１８０に対するコンテンツの販売業務および課金業務を管理する機能も有する。情報配信管理部４１０は，さらに，パッケージ化されたコンテンツを格納したり，あるいは販売業務や課金業務に関する履歴を格納するデータベース４６０を管理している。

【0074】（情報提供部４２０）情報提供部４２０は，パッケージが正規のオーサリングシステムにより作成されたものかどうかなどの検証動作や認証動作を行い，認証が肯定的である場合に，コンテンツをリーダ／ライタ（Ｒ／Ｗ）４３０を介してメモリスティックなどの記憶装置１８２への書き込みを行う機能を有している。

【0075】情報提供部４２０は，図９に示すように，外部認証部４２２と，内部認証部４２４と，再生制御部４２８とから主に成るソフトウェアとして構成することができる。

【0076】情報提供部４２０は，例えば，情報配布端末４００に組み込まれたＤＬＬ（Ｄｙｎａｍｉｃ　Ｌｉ

ｎｋ Ｌｉｂｒａｒｙ）として構成される。情報提供部４２０を，所定のＯＳ，例えばＷｉｎｄｏｗｓ２０００上で動作するアプリケーションとして組み込んだ一例を図１２に示す。なお，図１２に示す情報提供部４２０は，理解を容易にするために，ＧＵＩアプリケーション部４２９と，セキュアモジュール部４２５と，インタフェース部４２７とから構成している。

【００７７】（外部認証部４２２）再び図９を参照して，外部認証部４２２は，情報提供部４２０が正規のものであるか，すなわち情報配布端末４００が記憶しているコンテンツを外部に提供する権限を有するかどうかを，情報提供部４２０が予め保管する第１の外部認証鍵（Ｋａｕｔｈ（１））と，認証サーバ５００が保管する第２の外部認証鍵（Ｋａｕｔｈ（２））とを用いて，比較認証する機能を有している。

【００７８】外部認証は，情報提供部４２０を起動するたびに必ず行う必要がある。ただし，一度認証が通れば，情報提供部４２０の起動中は再度行わなくてもよい。

【００７９】外部認証部４２２は，図１０に示すように，外部認証管理部４２２１と，鍵保持手段４２２２と，乱数発生手段４２２３と，第１の暗号化手段４２２４と，第２の暗号化手段４２２５と，比較手段４２２６と，送受信手段４２２７とから主に構成されている。

【００８０】（外部認証管理部４２２１）外部認証管理部４２２１は，外部認証部４２２における認証動作を全体的に管理する。外部認証管理部４２２１は，情報提供部４２０が起動されると，後述する外部認証を行い，外部認証が成功すると，内部認証部４２４に処理を受け渡すように動作する。

【００８１】（鍵保持手段４２２２）鍵保持手段４２２２は，第１の外部認証鍵（Ｋａｕｔｈ（１））をセキュアに保持する。第１の外部認証鍵（Ｋａｕｔｈ（１））は，認証サーバ部５００から事前に，情報提供部４２０に配布されるが，この第１の外部認証鍵（Ｋａｕｔｈ（１））は，情報提供部４２０の認証部（セキュアモジュール）内にタンパレジスタント（Ｔａｍｐｅｒ Ｒｅｓｉｓｔａｎｔ）に隠蔽されているので，リバースエンジニアリングしても値を調べることが困難である。

【００８２】（乱数発生手段４２２３）乱数発生手段４２２３は，外部認証用の乱数を発生する。乱数発生手段４２２３で発生された乱数は，一方で，第１の暗号化手段４２２４に送られ第１の外部認証鍵（Ｋａｕｔｈ（１））により暗号化され第１の暗号化データを生成する。他方で，乱数発生手段４２２３で発生された乱数は，第２の暗号化手段４２２４に送られ第２の外部認証鍵（Ｋａｕｔｈ（２））により暗号化され第２の暗号化データを生成する。

【００８３】（第１の暗号化手段４２２４）第１の暗号化手段４２２４は，基本的には，情報提供部４２０内に組み込まれているソフトウェアである。第１の暗号化手段４２２４は，乱数発生手段４２２３が発生した乱数を，鍵保持手段４２２２にセキュアに保持された第１の外部認証鍵（Ｋａｕｔｈ（１））を用いて暗号化し第１の暗号化データを生成する。

【００８４】（第２の暗号化手段４２２５）第２の暗号化手段４２２５は，乱数発生手段４２２３が発生した乱数を，第１の暗号化手段４２２４とは別のルートで，第１の外部認証鍵（Ｋａｕｔｈ（１））と同一の第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて暗号化して第２の暗号化データを取得する。

【００８５】第２の暗号化手段４２２５による第２の暗号化データ取得の構成は，要求されるセキュリティレベルに応じて，さまざまな実施形態を採用可能である。

【００８６】（ローカル外部認証）最もセキュリティレベルが低い実施形態は，図１３に示すように，ローカルで，すなわち情報提供部４２０内において外部認証を行う。この実施形態においては，第２の暗号化手段４２２５も情報提供部４２０内に組み込まれ，情報提供部４２０内に事前に組み込まれた第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて乱数を暗号化して第２の暗号化データを取得する。

【００８７】しかしながら，かかるローカルな外部認証の態様では，情報配布端末４００を悪意に操作する者に第２の外部認証鍵（Ｋａｕｔｈ（２））が盗まれる可能性がある。また情報配布端末４００自体を盗まれた場合には，情報配布端末４００内に記憶されたパッケージのダウンロードが可能になってしまう。したがって，上記のようなローカルな外部認証は，情報配布端末自体を盗まれないように設計してある場合や，盗まれるとデータが破壊されるように設計している場合には有効である。なお，図１３に示す実施形態における外部認証動作については後述する。

【００８８】（リモート外部認証）これに対して，最もセキュリティレベルの高い実施形態は，図１４に示すように，リモートで，すなわち情報提供部４２０の外部にある認証サーバ５００を利用して外部認証を行う。この実施形態においては，認証サーバ部５００は，認証サーバ部５００内に上記乱数を取り込んで，第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて第２の暗号化データを生成する。

【００８９】したがって，第２の外部認証鍵（Ｋａｕｔｈ（２））が盗まれることがなく，また情報配布端末４００自体を盗まれた場合であっても，情報配布端末４００内に記憶されたパッケージのダウンロードを行うことはできない。なお，図１４に示す実施形態における外部認証動作については後述する。

【００９０】（セミローカル外部認証）さらに，図１３に示す実施形態と図１４に示す実施形態との中位のセキュリティレベルを有する実施形態を図１５に示す。この

実施形態においては，認証サーバ部５００は，必要に応じて，例えばダウンロードを行う際に，第２の外部認証鍵（Ｋａｕｔｈ（２））を情報提供部４２０に一時的に受け渡される。情報提供部４２０は認証サーバ部５００から受け渡された第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて乱数を暗号化し，第２の暗号化データを生成する。第２の暗号化データが生成された後に，あるいは情報配布端末４００への電源が遮断されるごとに，第２の外部認証鍵（Ｋａｕｔｈ（２））は情報提供部４２０から消去される。

【００９１】この実施形態によれば，ダウンロードなどの必要な時にのみ，第２の外部認証鍵（Ｋａｕｔｈ（２））が情報配布端末４００に一時的に受け渡されるので，第２の外部認証鍵（Ｋａｕｔｈ（２））自体の盗難による被害のおそれが著しく軽減される。また情報配布端末４００自体を盗まれた場合であっても，第２の外部認証鍵（Ｋａｕｔｈ（２））を，情報配布端末４００の電源が遮断された時点で消去されるように構成すれば，情報配布端末４００内に記憶されたパッケージのダウンロードを行うことはできない。なお，図１５に示す実施形態における外部認証動作については後述する。

【００９２】（比較手段４２２６）比較手段４２２６は，第１の暗号化手段４２２４が生成した第１の暗号化データと第２の暗号化手段４２２５が生成した第２の暗号化データとを比較する。比較の結果，第１の暗号化データと第２の暗号化データとが一致する場合に，外部認証が完了する。

【００９３】（送受信手段４２２７）送受信手段４２２７は，外部認証部４２２における情報の送受信を行う。送受信手段４２２７は，例えば，乱数発生手段４２２３が発生した乱数を外部に送信したり，認証サーバ５００などから第２の暗号化手段４２２５が取得した第２の暗号化データを取り込んだりする。

【００９４】（内部認証部４２４）内部認証部４２４は，情報提供部４２０の外部認証完了後に行われる内部認証を行う機能を有する。内部認証部４２４は，図１１に示すように，第１の認証手段４２４２と，第２の認証手段４２４４とから構成されている。

【００９５】（第１の認証手段４２４２）第１の認証手段４２４２は，配布対象であるコンテンツデータが，正規のオーサリングシステム（オーサリングスタジオ３００）により作成されたコンテンツであるかを認証するための手段を提供する。具体的には，第１の認証は，正規のオーサリングシステムが前記コンテンツデータに書き込んだＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）値を検証して行われる。

【００９６】ＭＡＣ値は，メインコンテンツに付随する付随データのうち利用条件情報をコンテンツ鍵（Ｋｃ）を用いて計算される。そのため，ＭＡＣ値は，コンテンツ鍵（Ｋｃ）およびルート鍵（Ｋｒｏｏｔ）を知らないと計算することができないため，情報提供部４２０とオーサリング鍵（ＣＥＤ）を供給された者でないとパッケージデータを作成できない。

【００９７】（第２の認証手段４２４４）第２の認証手段４２４４は，記録手段であるリーダ／ライタ４３０と情報記録管理手段である情報提供装置４２０との相互認証を行うための手段を提供する。第２の認証手段４２４４は，まず，正規のオーサリングシステム３００がルート鍵（Ｋｒｏｏｔ）をデバイス鍵（Ｋｄｅｖｉｃｅ）で暗号化したコンテンツ使用可能化鍵（ＥＫＢ）を，リーダ／ライタ４３０と情報提供装置４２０との双方に受け渡す。リーダ／ライタ４３０と情報提供装置４２０は，それぞれがセキュアに保持するデバイス鍵（Ｋｄｅｖｉｃｅ）を用いてルート鍵（Ｋｒｏｏｔ）を復号化させる。そして，復号化されたルート鍵（Ｋｒｏｏｔ）が相互に一致する場合に肯定的な認証を行う。

【００９８】（再生制御部４２８）再生制御部４２８は，内部認証の結果，ルート鍵（Ｋｒｏｏｔ）の共有が認証されたメモリスティックなどの所定の記憶媒体においてコンテンツデータを再生可能とするものである。再生制御部４２８は，リーダ／ライタ４３０が記憶媒体に複数のコンテンツデータを一括して記録する場合には，複数のコンテンツ全ての記録が終了した後に，複数のコンテンツの再生を可能とするように構成されている。

【００９９】（リーダ／ライタ（Ｒ／Ｗ）４３０）リーダ／ライタ（Ｒ／Ｗ）４３０は，メモリスティック，メモリカード，スマートメディアなどの記憶媒体に，コンテンツをダウンロードするためのハードウェアである。すでに説明したように，ダウンロードを行う前に，情報提供部４２０とリーダ／ライタ（Ｒ／Ｗ）４３０間において，内部認証を行い，相互に正規の装置であることを確認した上で，ダウンロードを行う。

【０１００】（販売管理部４４０）販売管理部４４０は，パッケージ化されたコンテンツの販売時に生じる様々業務を管理する。販売管理部４４０は，さらに，販売履歴を管理して，販売情報を収集する。販売管理部４４０は，例えば，どの時間帯に，どのような年齢層の男性または女性に，どの程度の値段の，どのようなジャンルのコンテンツが，どの程度の数量販売されたかなどについての統計的情報を収集し，将来的な商品開発に役立てることができる。

【０１０１】（課金制御部４５０）課金制御部４５０は，パッケージ化されたコンテンツの販売時に生じる課金ベースの業務を管理する。課金制御部４５０は，例えばユーザが現金で支払を行う場合には，つり銭などの精算業務を管理する。課金制御部４５０は，例えばユーザがクレジットカードなどで支払を行う場合には，本人照合や信用照会などの業務を管理する。

【０１０２】データベース４６０は，情報配信端末４００に関連する各種情報を格納し管理する。データベース

４６０には，例えば，本実施の形態にかかる情報配布システム１００の配布対象であるパッケージ化されたコンテンツや，販売履歴や課金履歴などの各種履歴情報などが格納されている。

【０１０３】（２．２．４　認証サーバ部５００）認証サーバ部５００は，ある情報配信端末４００がコンテンツのダウンロードを行う権限を有する正規の情報配信端末であるか外部認証を行う機能を有している。本実施の形態にかかる情報配信システム１００においては，情報配信端末４００は，所定のパッケージ化されたコンテンツをダウンロードする前に，所定の記憶媒体にダウンロード許可権限を有する情報提供部４２０が正規の装置であるか否かを外部認証する必要がある。

【０１０４】認証サーバ部５００は，情報提供部４２０の外部認証を行う機能を有している。外部認証は，後述するように，一方で，情報提供部４２０内において，乱数発生手段４２３により発生された乱数を鍵保持手段４２２内にセキュアに保持された第１の外部認証鍵（Ｋａｕｔｈ（１））を用いて暗号化し，第１の暗号化データを生成する。第１の外部認証鍵（Ｋａｕｔｈ（１））は，認証サーバ部５００から事前に，情報提供部４２０に配布されるが，この第１の外部認証鍵（Ｋａｕｔｈ（１））は，情報提供部４２０の認証部（セキュアモジュール）内にタンパレジスタント（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ）に隠蔽されているので，リバースエンジニアリングしても値を調べることは困難である。

【０１０５】他方，別のルートで，第１の外部認証鍵（Ｋａｕｔｈ（１））と同一の第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて同様の乱数を暗号化して第２の暗号化データを取得する。そして，情報提供部４２０内において発生された第１の暗号化データと，第１の暗号化データとは別ルートで生成された第２の暗号化データとを比較し，両者が一致した場合に，情報提供部４２０が正規のものであると外部認証するように構成されている。

【０１０６】認証サーバ部５００は，基本的には，上記外部認証工程において，第２の外部認証鍵（Ｋａｕｔｈ（２））を管理している。後述するように，ある実施形態においては，認証サーバ部５００は，認証サーバ部５００内に上記乱数を取り込んで第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて第２の暗号化データを生成する。別の実施形態においては，認証サーバ部５００は，第２の外部認証鍵（Ｋａｕｔｈ（２））を情報提供部４２０に受け渡して第２の暗号化データを生成する。なお，第２の外部認証鍵（Ｋａｕｔｈ（２））を情報提供部４２０内にセキュアに保持する別の実施形態においては，認証サーバ部５００が事前に第２の外部認証鍵（Ｋａｕｔｈ（２））に配布する。

【０１０７】なお，認証サーバ部５００が管理する第１および第２の外部認証鍵（Ｋａｕｔｈ（１））（２）の発行および管理に関しては，権限のある鍵管理装置１６０に委託することが可能である。鍵管理装置１６０は，第１および第２の外部認証鍵（Ｋａｕｔｈ（１））（２）を発行するのみならず，例えば，情報配信端末４００が盗難にあったような場合には，第１および第２の外部認証鍵（Ｋａｕｔｈ（１））（２）の内容を更新し，盗まれた情報配信端末４００の情報提供部４２０を無効化することが可能である。

【０１０８】（２．２．５　ネットワーク部６００）ネットワーク部６００は，オーサリングスタジオ３００においてパッケージ化されたコンテンツを情報配信端末４００に配信する通信網である。ネットワーク部６００は，衛星通信網のような無線通信網６００ａと，専用回線網６００ｂの双方を含んでいる。セキュリティを確保するためには，ネットワーク部６００は，閉鎖系である専用回線網６００ｂから構成することが好ましいが，もちろん，インターネットなどの開放系のネットワークとして構成しても構わない。また，多数の情報配信端末４００に同時に配信を行うのであれば，衛星通信網のような無線通信網６００ａの利用が好適である。

【０１０９】（２．３　鍵管理装置）鍵管理装置１６０は，本実施の形態にかかる情報配信システムの各段階において利用される鍵を管理する権限のある管理者である。鍵管理装置１６０は，オーサリング装置３１６に対してはオーサリング鍵生成装置として機能する。ここで管理される鍵および鍵関連情報は以下の通りである。また，鍵情報は，定期的にまたは必要に応じて更新され，環境変化に対応するとともに，セキュリティの向上が図られる。

【０１１０】（２．３．１　オーサリングスタジオ３００において使用される鍵情報）「コンテンツ鍵（Ｋｃ）」は，オーサリングスタジオ３００において，コンテンツを暗号化する際に使用される鍵である。コンテンツ鍵（Ｋｃ）はルート鍵（Ｋｒｏｏｔ）により暗号化され，ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）に加工される。

【０１１１】「コンテンツ識別子（ＣＩＤ）」は，コンテンツ毎に割り振られる識別子である。コンテンツＩＤ（ＣＩＤ）は，各コンテンツに固有の識別子であり，重複して設定されることはない。コンテンツ識別子（ＣＩＤ）の生成は，オーサリング作業の現場ではなく，オーサリング鍵生成装置１６０において管理するので，コンテンツ識別子（ＣＩＤ）のユニーク性を完全に保証することができる。

【０１１２】「ルート鍵（Ｋｒｏｏｔ）」は，コンテンツ鍵（Ｋｃ）を暗号化する際に使用される鍵である。ルート鍵（Ｋｒｏｏｔ）は，「コンテンツ鍵暗号化鍵」とも称されることがある。共通に使用されるルート鍵（Ｋｒｏｏｔ）は非常に重要な鍵であるが，本システムによれば，このルート鍵（Ｋｒｏｏｔ）をオーサリング装置

３１６に直接渡すことなく，コンテンツ鍵（Ｋｃ），ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）のセットをオーサリング鍵（ＣＥＤ）としてオーサリング装置３１６に渡すことにより，セキュリティを向上させるとともに，組み合わせの間違いを防止することができる。

【０１１３】「ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）」は，コンテンツ鍵（Ｋｃ）をルート鍵（Ｋｒｏｏｔ）で暗号化したものである。ＥＫｃ＝Ｅ（Ｋｒｏｏｔ，Ｋｃ）と表現できる。コンテンツ鍵（Ｋｃ）とルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）とをセットにしてオーサリング鍵（ＣＥＤ）として生成することにより，組み合わせの間違いを回避できる。

【０１１４】「デバイス鍵（Ｋｄｅｖｉｃｅ）」は，パッケージ化されたコンテンツを利用可能な再生装置に関する鍵情報である。デバイス鍵は，各再生装置がハードウェア的にあるいはタンパレジスタントソフトにより，セキュアに保持している鍵情報である。

【０１１５】「コンテンツ使用可能化鍵（ＥＫＢ：Ｅｎａｂｌｉｎｇ Ｋｅｙ Ｂｌｏｃｋ」は，ルート鍵（Ｋｒｏｏｔ）をデバイス鍵（Ｋｄｅｖｉｃｅ）で暗号化したものである。コンテンツ使用可能化鍵（ＥＫＢ）には，Ｅ（ＫｄｅｖｉｃｅＡ，Ｋｒｏｏｔ），Ｅ（ＫｄｅｖｉｃｅＢ，Ｋｒｏｏｔ）といったデータが格納されており，再生装置Ａ（ＤｅｖｉｃｅＡ）は，Ｅ（ＫｄｅｖｉｃｅＡ，Ｋｒｏｏｔ）を解くことによりＫｒｏｏｔを知ることが可能である。同様に，再生装置Ｂ（ＤｅｖｉｃｅＢ）は，Ｅ（ＫｄｅｖｉｃｅＢ，Ｋｒｏｏｔ）を解くことによりＫｒｏｏｔを知ることが可能である。

【０１１６】「オーサリング鍵使用鍵（ＣＥＫ（Ｃｏｎｔｅｎｔ Ｅｎａｂｌｉｎｇ Ｋｅｙ））は，コンテンツをオーサリングする事業者と管理者との間で共有される共有秘密情報（鍵）である。オーサリングする事業者毎に異なり，管理者によって発行され管理される。オーサリングする際に，オーサリング鍵（ＣＥＤ）と共に用いられる。

【０１１７】「オーサリング鍵（ＣＥＤ（Ｃｏｎｔｅｎｔ Ｅｎａｂｌｉｎｇ Ｄａｔａ））は，コンテンツをオーサリングする時に使用される鍵である。権限のある管理者によって発行され管理される。コンテンツＩＤ（ＣＩＤ）と関連付けされており，一つのコンテンツに一つのオーサリング鍵（ＣＥＤ）を用いてオーサリングを行う。オーサリング鍵は，コンテンツ鍵（Ｋｃ）およびルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）をコンテンツＩＤ（ＣＩＤ）とオーサリング鍵使用鍵（ＣＥＫ）で暗号化したものである。

【０１１８】「冗長コンテンツ鍵ブロック（ＲＫｃＢ（Ｒｅｄｕｎｄａｎｔ Ｋｃ Ｂｌｏｃｋ））」は，オーサリング鍵（ＣＥＤ）の中に含まれるべき，コンテンツ鍵（Ｋｃ），ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ），コンテンツ使用可能化鍵のバージョン情報（ＥＫＢ－Ｖｅｒｓｉｏｎ）を連結し，さらに不正な解読を困難とするために冗長な乱数情報を付加したデータブロックである。オーサリング鍵（ＣＥＤ）を生成する際に，その生成過程で生成する。オーサリング鍵（ＣＥＤ）を生成する処理過程で使用するデータで，ユーザやアプリケーション開発者には意識されない。

【０１１９】「チェックサム付冗長コンテンツ鍵ブロック（ＣＲＫｃＢ）」は，冗長コンテンツ鍵ブロック（ＲＫｃＢ）のチェックサム（ＣＳ）を計算し，冗長コンテンツ鍵ブロック（ＲＫｃＢ）に連結して得られるデータブロックである。

【０１２０】「最終暗号化鍵（Ｋｃｉｄ）」は，オーサリング鍵（ＣＥＤ）作成フローにおいて，最後の暗号化に使用する鍵データである。コンテンツＩＤ（ＣＩＤ）とオーサリング鍵使用鍵（ＣＥＫ）から生成される。最終暗号化鍵（Ｋｃｉｄ）自体は，オーサリング鍵（ＣＥＤ）を生成する処理過程使用するデータであるので，ユーザやアプリケーション開発者には意識されない。オーサリング鍵（ＣＥＤ）を使用する際には，コンテンツＩＤ（ＣＩＤ）とオーサリング鍵使用鍵（ＣＥＫ）が分かれば，モジュール内部でＫｃｉｄを生成することにより，オーサリング鍵（ＣＥＤ）に含まれるコンテンツ鍵（Ｋｃ），ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ），コンテンツ使用可能化鍵のバージョン情報（ＥＫＢ－Ｖｅｒｓｉｏｎ）を獲得することができる。

【０１２１】（２．３．２ 情報配信端末４００において使用される鍵情報および鍵関連情報）情報配信端末４００においては，暗号化コンテンツデータの（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））復号時，外部認証時，内部認証時に，それぞれ鍵情報および鍵関連情報が使用される。

【０１２２】（復号時に使用される情報）「暗号化コンテンツデータ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ））」は，デバイス鍵（Ｋｄｅｖｉｃｅ）およびコンテンツ使用可能化鍵（ＥＫＢ），第２のコンテンツ鍵（ＥＫｃ）から獲得されるコンテンツ鍵（Ｋｃ）を利用して復号化される。

【０１２３】「デバイス鍵（Ｋｄｅｖｉｃｅ）」は，パッケージ化されたコンテンツを利用可能な再生装置に関する鍵情報である。デバイス鍵は，各再生装置がハードウェア的にあるいはタンパレジスタントソフトにより，セキュアに保持している鍵情報である。

【０１２４】「コンテンツ使用可能化鍵（ＥＫＢ）」は，ルート鍵（Ｋｒｏｏｔ）をデバイス鍵（Ｋｄｅｖｉｃｅ）で暗号化したものである。コンテンツ使用可能化鍵（ＥＫＢ）には，Ｅ（ＫｄｅｖｉｃｅＡ，Ｋｒｏｏｔ），Ｅ（ＫｄｅｖｉｃｅＢ，Ｋｒｏｏｔ）といったデータが格納されており，再生装置Ａ（ＤｅｖｉｃｅＡ）は，Ｅ（ＫｄｅｖｉｃｅＡ，Ｋｒｏｏｔ）を解くことに

よりＫｒｏｏｔを知ることが可能である。同様に，再生装置Ｂ（ＤｅｖｉｃｅＢ）は，Ｅ（ＫｄｅｖｉｃｅＢ，Ｋｒｏｏｔ）を解くことによりＫｒｏｏｔを知ることが可能である。

【０１２５】（外部認証時に使用される鍵情報）情報提供部４２０の外部認証時には，第１の外部認証鍵（Ｋａｕｔｈ（１））と第２の外部認証鍵（Ｋａｕｔｈ（２））が使用される。

【０１２６】「第１の外部認証鍵（Ｋａｕｔｈ（１））」は，認証サーバ部５００から事前に，情報提供部４２０に配布される外部認証鍵である。この第１の外部認証鍵（Ｋａｕｔｈ（１））は，情報提供部４２０の認証部（セキュアモジュール）内にタンパレジスタント（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ）に隠蔽されているので，リバースエンジニアリングしても値を調べることは困難である。第１の外部認証鍵（Ｋａｕｔｈ（１））は，第１の暗号化手段４２２４が乱数を暗号化して第１の暗号化データを生成する際に用いられる。

【０１２７】「第２の外部認証鍵（Ｋａｕｔｈ（２））」は，認証サーバ部５００により発行される第１の外部認証鍵（Ｋａｕｔｈ（１））と同一の鍵である。第２の外部認証鍵（Ｋａｕｔｈ（２））は，第２の暗号化手段４２２５が乱数を暗号化して第２の暗号化データを生成する際に用いられる。

【０１２８】（内部認証時に使用される鍵情報）情報提供部４２０の内部認証時には，情報提供部４２０とリーダ／ライタ４９０とがそれぞれ有するデバイス鍵（Ｋｄｅｖｉｃｅ）でコンテンツ使用可能化鍵（ＥＫＢ）を復号して得られたルート鍵（Ｋｒｏｏｔ）が参照される。

【０１２９】（２．４　ユーザ部）ユーザ部１８０は，キオスク端末などの情報配布端末４００にアクセスし，気に入ったコンテンツをダウンロードする機能を有しているコンピュータ装置などの情報処理端末である。

【０１３０】ユーザ部１８０は，図１に示すように，メモリスティックなどの記憶媒体１８２と再生装置１８４を主な構成要素としている。さらに，ユーザ部１８０は，他の記憶媒体および／または再生装置１８６を備える場合もあり，許可された回数内で，記憶媒体１８２にダウンロードしたコンテンツを，他の記憶媒体および／または再生装置１８６に対して，チェックアウトまたはムーブすることが可能である。

【０１３１】（３　オーサリング動作）次に，オーサリングスタジオ３００におけるオーサリング動作について説明する。本実施の形態にかかる情報配信システム１００においては，オーサリング時にコンテンツの暗号化とパッケージ化を行うこと，およびオーサリング鍵を生成するオーサリング鍵生成装置１６０と実際にオーサリング鍵を用いてコンテンツの暗号化を行うオーサリング装置３１６とを別構成にしたこと，さらに，ルート鍵を直接オーサリング装置３１６に渡さずにコンテンツの暗号化を可能にしたことなどを特徴としている。

【０１３２】また，オーサリングを行う際に，オーサリング鍵の内容は知る必要が無いため，オーサリング鍵の生成とオーサリング作業を完全に分離することが可能である。さらに，オーサリング作業とオーサリング鍵生成を分離することにより，オーサリング作業で正しく生成できるパッケージの数を，オーサリング作業の外で制御することが可能である。

【０１３３】さらに，オーサリング鍵生成時に使用する暗号化の鍵として，コンテンツ識別子（ＣＩＤ）に加えてオーサリング鍵生成時に任意に指定できるオーサリング鍵使用鍵（ＣＥＫ）を付加することにより，生成したオーサリング鍵を正しく使用できる人をオーサリング鍵使用鍵（ＣＥＫ）を知っている人に限定することができる。

【０１３４】さらに，オーサリング時に設定した，利用条件等の内容に対して，正しいシステムのみ知り得る鍵を使用したＭＡＣ値を付加することにより，パッケージの改ざんを防止することができる。

【０１３５】（３．１　オーサリング鍵の生成動作）オーサリング鍵生成装置（鍵管理装置）１６０におけるオーサリング鍵の生成動作について説明する。

【０１３６】オーサリング鍵（ＣＥＤ）には，基本的に，コンテンツ鍵（Ｋｃ），ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）の情報が含まれる。なお，ＥＫｃは，Ｅ（Ｋｒｏｏｔ，Ｋｃ）と表現することが可能である。また，ルート鍵（Ｋｒｏｏｔ）は，コンテンツ鍵（Ｋｃ）を暗号化するために使用される鍵であり，セキュリティのために非常に重要な鍵である。後述するように，本システムによれば，共通に使用されるルート鍵（Ｋｒｏｏｔ）をオーサリング装置３１６に直接渡すことなく，コンテンツ鍵（Ｋｃ），ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）のセットをオーサリング鍵（ＣＥＤ）としてオーサリング装置３１６に渡すことにより，セキュリティを向上させるとともに，組み合わせの間違いを防止することができる。

【０１３７】図１７（１）に示すように，オーサリング鍵（ＣＥＤ）は，コンテンツデータを暗号化するためのコンテンツ鍵（Ｋｃ）とルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）を，コンテンツデータ毎にユニークに割り当てられるコンテンツ識別子（ＣＩＤ）とオーサリング装置３１６毎にユニークに割り当てられるオーサリング鍵使用鍵（ＣＥＫ）で暗号化したものである。

【０１３８】図６に示すオーサリング鍵生成手段１６６において，オーサリング鍵（ＣＥＤ）の生成に必要となるものは，コンテンツ識別子生成手段１６２により生成されたコンテンツ識別子（ＣＩＤ）と，コンテンツ鍵（Ｋｃ），ルート鍵（Ｋｒｏｏｔ）で暗号化したコンテンツ鍵（ＥＫｃ）と，オーサリング鍵使用鍵生成手段１６４によりオーサリング鍵使用鍵（ＣＥＫ）である。

【０１３９】図１６に，オーサリング鍵生成手段１６６において実施されるオーサリング鍵（ＣＥＤ）の生成工程の詳細なフローを示す。

【０１４０】まず，ステップＳ１６０２において，オーサリング鍵（ＣＥＤ）の中に含まれるべき，コンテンツ鍵（Ｋｃ），ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ），コンテンツ使用可能化鍵のバージョン情報（ＥＫＢ－Ｖｅｒｓｉｏｎ）を連結し，さらに不正な解読を困難とするために冗長な乱数情報を付加したデータブロックである，冗長コンテンツ鍵ブロック（ＲＫｃＢ（ＲｅｄｕｎｄａｎｔＫｃ　Ｂｌｏｃｋ））を生成する。

【０１４１】なお，コンテンツ使用可能化鍵（ＥＫＢ）は，ルート鍵（Ｋｒｏｏｔ）をデバイス鍵（Ｋｄｅｖｉｃｅ）で暗号化したものであり，コンテンツ使用可能化鍵のバージョン情報（ＥＫＢ－Ｖｅｒｓｉｏｎ）は，コンテンツ使用可能化鍵のバージョン情報である。このように，あるコンテンツ鍵（Ｋｃ）に対して特定されるべきルート鍵（Ｋｒｏｏｔ）のバージョン（Ｖｅｒｓｉｏｎ）を示す情報をもセットにすることにより，コンテンツ鍵（Ｋｃ），ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ），ルート鍵（Ｋｒｏｏｔ）の組み合わせの間違いを防ぐことができる。

【０１４２】次いでステップＳ１６０４において，冗長コンテンツ鍵ブロック（ＲＫｃＢ）のチェックサム（ＣＳ）を計算し，例えば，チェックサム（ＣＳ）を冗長コンテンツ鍵ブロック（ＲＫｃＢ）の後ろに連結することによりチェックサム付冗長コンテンツ鍵ブロック（ＣＲＫｃＢ）を獲得する。

【０１４３】このようにオーサリング鍵（ＣＥＤ）を生成する過程において，コンテンツ鍵（Ｋｃ）とルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）以外にチェックサム情報を負荷することにより，誤ったコンテンツ識別子（ＣＩＤ）によるオーサリング鍵（ＣＥＤ）による使用を非常に高い確率で防止することができる。

【０１４４】次いでステップＳ１６０６において，コンテンツ識別子（ＣＩＤ）とオーサリング鍵使用鍵（ＣＥＫ）から最終暗号化鍵（Ｋｃｉｄ）を生成する。図１７（２）に関連して後述するように，オーサリング鍵（ＣＥＤ）を使用する際には，コンテンツＩＤ（ＣＩＤ）とオーサリング鍵使用鍵（ＣＥＫ）が分かれば，モジュール内部でＫｃｉｄを生成することにより，オーサリング鍵（ＣＥＤ）に含まれるコンテンツ鍵（Ｋｃ），ルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ），コンテンツ使用可能化鍵のバージョン情報（ＥＫＢ－Ｖｅｒｓｉｏｎ）を獲得することができる。

【０１４５】ここで，最終暗号化鍵（Ｋｃｉｄ）を生成する過程において，コンテンツ毎にユニークなコンテンツ識別子（ＣＩＤ）を使用することにより，オーサリング鍵による暗号化作業の際に，正しいコンテンツ識別子（ＣＩＤ）を使用した場合に正しいオーサリング作業が可能となるので，オーサリングの精度を高めることが可能となる。また，コンテンツ識別子（ＣＩＤ）の生成を，オーサリング鍵生成装置１６０において管理することにより，コンテンツ識別子（ＣＩＤ）のユニーク性を完全に保証することができる。

【０１４６】最後にステップＳ１６０８において，チェックサム付冗長コンテンツ鍵ブロック（ＣＲＫｃＢ）を最終暗号化鍵（Ｋｃｉｄ）で暗号化することによりオーサリング鍵（ＣＥＤ）を生成する。

【０１４７】（３．２　オーサリング鍵による暗号化動作）次に，図１８を参照しながら，オーサリング鍵生成装置（鍵管理装置）１６０において生成されたオーサリング鍵によるコンテンツの暗号化動作について説明する。

【０１４８】まずステップＳ１９０２に示すように，オーサリング装置３１６のコンテンツ鍵復号化手段３１６２は，オーサリング鍵生成装置（鍵管理装置）１６０から共有秘密鍵であるオーサリング鍵使用鍵（ＣＥＫ）を取得する。なお，以下において，オーサリング鍵を生成するオーサリング鍵生成装置とオーサリング鍵などの鍵情報を管理する鍵管理装置を同一の装置として説明するが，オーサリング鍵生成装置と鍵管理装置とは別体に構成しても構わない。

【０１４９】次いで，ステップＳ１９０４において，コンテンツ鍵復号化手段３１６２は，オーサリング鍵生成装置（鍵管理装置）１６０からオーサリングするコンテンツ用にコンテンツ識別子（ＣＩＤ）とオーサリング鍵（ＣＥＤ）のペアを取得する。

【０１５０】ステップＳ１９０２およびＳ１９０４に関して，オーサリング鍵（ＣＥＤ）は，コンテンツ識別子（ＣＩＤ）とオーサリング鍵（ＣＥＤ）のペアと同じタイミングで取得する必要は無い。コンテンツ識別子（ＣＩＤ）とオーサリング鍵（ＣＥＤ）のペアはコンテンツ毎に異なるが，オーサリング鍵使用鍵（ＣＥＫ）はオーサリング装置３１６にユニークな値なので，オーサリング処理に先立って一度取得しておけばよい。

【０１５１】また，コンテンツ識別子（ＣＩＤ）とオーサリング鍵（ＣＥＤ）のペアに関しても，各コンテンツをオーサリングする度にその都度取得する必要はない。複数のコンテンツをオーサリングする場合には，一括取得するように構成しても構わない。

【０１５２】次いで，ステップＳ１９０６において，コンテンツ鍵復号化手段３１６２は，図１７（２）に示すように，オーサリング鍵（ＣＥＤ）から，コンテンツ識別子（ＣＩＤ）とオーサリング鍵使用鍵（ＣＥＫ）を用いて，コンテンツ鍵（Ｋｃ）とルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）とを復号化する。

【０１５３】次いで，ステップＳ１９０８において，オーサリング装置３１６のコンテンツ暗号化手段３１６４

は，コンテンツ鍵復号化手段３１６２により復号化したコンテンツ鍵（Ｋｃ）を用いてコンテンツデータを暗号化して暗号化コンテンツデータＥ（Ｋｃ，Ｃｏｎｔｅｎｔ）を生成する。

【０１５４】次いで，ステップＳ１９１０において，パッケージ手段３１６６により，暗号化コンテンツデータＥ（Ｋｃ，Ｃｏｎｔｅｎｔ）とともに，コンテンツ識別子（ＣＩＤ）とルート鍵で暗号化した第２のコンテンツ鍵（ＥＫｃ）とをパッケージ化して一連のオーサリング作業を終了する。

【０１５５】（４　情報配信動作）以上のようにしてオーサリング処理が終了したコンテンツは，図１に示すように所定のネットワーク６００を介してキオスク端末などの情報配信端末４００に送信される。情報配信端末４００には，図１９に示すように，暗号化コンテンツ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ）），ルート鍵で暗号化されたコンテンツ鍵（ＥＫｃ）およびコンテンツ使用可能化鍵（ＥＫＢ）が送られる。なお，暗号化コンテンツＥ（Ｋｃ，Ｃｏｎｔｅｎｔ）のヘッダ部には，改ざん防止用に，コンテンツ鍵Ｋｃを用いて計算したＭＡＣ値が付加される。

【０１５６】情報配信端末４００においては，外部認証および内部認証から成る所定の認証動作が完了した後に，復号化処理がなされ，所定の記憶媒体１８２にダウンロードが行われる。以下，図２０に示すフローに沿って情報配信動作の詳細について説明する。

【０１５７】（４．１　外部認証動作）すでに説明したように，情報配信端末４００の外部認証部４２２は，情報提供部４２０が正規のものであるか，すなわち情報配布端末４００が記憶しているコンテンツを外部に提供する権限を有するかどうかを，情報提供部４２０が予め保管する第１の外部認証鍵（Ｋａｕｔｈ（１））と，認証サーバ５００が保管する第２の外部認証鍵（Ｋａｕｔｈ（２））とを用いて，比較認証する（ステップＳ２１０２）。ステップＳ２１０２において，外部認証に成功すれば，ステップＳ２１０４以下において行われる内部認証に進むが，外部認証に失敗すれば，コンテンツの情報配信（ＤＬ）動作は拒絶される（ステップＳ２１１２）。

【０１５８】外部認証は，情報提供部４２０を起動するたびに必ず行う必要がある。ただし，一度認証が通れば，情報提供部４２０の起動中は再度行わなくてもよい。

【０１５９】なお外部認証は，要求されるセキュリティレベルに応じて，第２の暗号化手段４２２５による第２の暗号化データ取得の態様を変更することにより，さまざまな実施形態を採用可能である。

【０１６０】（４．１．１　ローカル外部認証動作）最もセキュリティレベルが低い実施形態は，図１８に示すように，ローカルで，すなわち情報提供部４２０内において外部認証を行う。この実施形態においては，第２の外部認証鍵（Ｋａｕｔｈ（２））が情報提供部４２０内のアプリケーション内に組み込まれている。

【０１６１】まず第１の外部認証鍵（Ｋａｕｔｈ（１））をセキュアに保持するセキュアモジュール４２５は，乱数発生手段４２２３により生成した乱数を第１の外部認証鍵（Ｋａｕｔｈ（１））により暗号化し，第１の暗号化データを得る。

【０１６２】乱数発生手段４２２３により発生された乱数は，アプリケーションインタフェース４２３介してアプリケーション４２１に送られる。アプリケーション４２１は，予め記憶している第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて乱数を暗号化し，第２の暗号化データを得る。

【０１６３】第２の暗号化データは，アプリケーションインタフェース４２３を介して，セキュアモジュール４２５に戻される。セキュアモジュール４２５内において，第１の暗号化データと第２の暗号化データとが比較され，両者が一致した場合に，本実施の形態にかかる外部認証作業が終了する。

【０１６４】しかしながら，かかるローカル外部認証の態様では，情報配布端末４００を悪意に操作する者に第２の外部認証鍵（Ｋａｕｔｈ（２））が盗まれる可能性がある。また情報配布端末４００自体を盗まれた場合には，情報配布端末４００内に記憶されたパッケージのダウンロードが可能になってしまう。

【０１６５】（４．１．２　リモート外部認証動作）これに対して，最もセキュリティレベルの高い実施形態は，図１４に示すように，リモートで，すなわち情報提供部４２０の外部にある認証サーバ５００を利用して外部認証を行う。

【０１６６】まず第１の外部認証鍵（Ｋａｕｔｈ（１））をセキュアに保持するセキュアモジュール４２５は，乱数発生手段４２２３により発生した乱数を第１の外部認証鍵（Ｋａｕｔｈ（１））により暗号化し，第１の暗号化データを得る。

【０１６７】乱数発生手段４２２３により発生された乱数は，アプリケーションインタフェース４２３，アプリケーション４２１を介して認証サーバ部５００に送られる。認証サーバ部５００は，認証サーバ部５００内に上記乱数を取り込んで，第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて第２の暗号化データを生成する。

【０１６８】第２の暗号化データは，アプリケーションインタフェース４２３を介して，セキュアモジュール４２５に戻される。セキュアモジュール４２５内において，第１の暗号化データと第２の暗号化データとが比較され，両者が一致した場合に，本実施の形態にかかる外部認証作業が終了する。

【０１６９】このように本実施の形態にかかる外部認証動作によれば，第２の外部認証鍵（Ｋａｕｔｈ（２））

が盗まれることがなく，また情報配布端末４００自体を盗まれた場合であっても，情報配布端末４００内に記憶されたパッケージのダウンロードを行うことはできない。

【０１７０】（４．１．３　セミローカル外部認証動作）さらに，図１３に示す実施形態と図１４に示す実施形態との中位のセキュリティレベルを有する実施形態を図１５に示す。この実施形態においては，認証サーバ部５００は，必要に応じて，例えばダウンロードを行う際に，第２の外部認証鍵（Ｋａｕｔｈ（２））を情報提供部４２０に一時的に受け渡される。

【０１７１】まず第１の外部認証鍵（Ｋａｕｔｈ（１））をセキュアに保持するセキュアモジュール４２５は，乱数発生手段４２２３により発生された乱数を第１の外部認証鍵（Ｋａｕｔｈ（１））により暗号化し，第１の暗号化データを得る。

【０１７２】乱数発生手段４２２３により発生された乱数は，アプリケーションインタフェース４２３介してアプリケーション４２１に送られる。アプリケーション４２１は，予め記憶している第２の外部認証鍵（Ｋａｕｔｈ（２））を用いて乱数を暗号化し，第２の暗号化データを得る。

【０１７３】ここで，第２の外部認証鍵（Ｋａｕｔｈ（２））は認証サーバ部５００が管理しており，情報提供部４２０を起動する度に，アプリケーション４２１は認証サーバ部５００から第２の外部認証鍵（Ｋａｕｔｈ（２））を受け取り，乱数に対して暗号化処理を行う。第２の暗号化データが生成された後に，あるいは情報配布端末４００への電源が遮断されるごとに，第２の外部認証鍵（Ｋａｕｔｈ（２））は情報提供部４２０から消去される。

【０１７４】第２の暗号化データは，アプリケーションインタフェース４２３を介して，セキュアモジュール４２５に戻される。セキュアモジュール４２５内において，第１の暗号化データと第２の暗号化データとが比較され，両者が一致した場合に，本実施の形態にかかる外部認証作業が終了する。

【０１７５】この実施形態によれば，ダウンロードなどの必要な時にのみ，第２の外部認証鍵（Ｋａｕｔｈ（２））が情報配布端末４００に一時的に受け渡されるので，第２の外部認証鍵（Ｋａｕｔｈ（２））自体の盗難の可能性が著しく軽減される。また情報配布端末４００自体を盗まれた場合であっても，第２の外部認証鍵（Ｋａｕｔｈ（２））が情報配布端末４００の電源を遮断した時点で消去されてしまう構成を採用すれば，情報配布端末４００内に記憶されたパッケージのダウンロードを行うことはできない。

【０１７６】（４．２　内部認証動作）内部認証部４２４による内部認証動作は，情報提供装置４２０の外部認証完了後に行われる。内部認証動作は，第１の認証手段４２４２によって行われるコンテンツの検証動作（第１の認証動作）と，第２の認証手段４２４４によって行われる第２の認証動作とから構成されている。

【０１７７】図２０のステップＳ２１０４に示すコンテンツの検証動作は，配布対象であるコンテンツデータが，正規のオーサリングシステム（オーサリングスタジオ３００）により作成されたコンテンツであるかを検証するための手段を提供する。具体的には，第１の認証は，正規のオーサリングシステムが前記コンテンツデータに書き込んだＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を参照して行われる。ステップＳ２１０４において，コンテンツの検証に成功すれば，ステップＳ２１０６において行われる第２の内部認証に進むが，コンテンツの検証に失敗すれば，コンテンツの情報配信（ＤＬ）動作は拒絶される（ステップＳ２１１２）。

【０１７８】ステップＳ２１０６において，第２の認証手段４２４４は，記録手段であるリーダ／ライタ４３０と情報記録管理手段である情報提供装置４２０との相互認証を行うための手段を提供する。第２の認証手段４２４４は，まず，正規のオーサリングシステム３００が，ルート鍵（Ｋｒｏｏｔ）をデバイス鍵（Ｋｄｅｖｉｃｅ）で暗号化したコンテンツ使用可能化鍵（ＥＫＢ）を，リーダ／ライタ４３０と情報提供装置４２０との双方に受け渡す。リーダ／ライタ４３０と情報提供装置４２０は，それぞれがセキュアに保持するデバイス鍵（Ｋｄｅｖｉｃｅ）を用いてルート鍵（Ｋｒｏｏｔ）を復号化させる。そして，復号化されたルート鍵（Ｋｒｏｏｔ）が相互に一致する場合に肯定的な認証を行う。ステップＳ２１０６において，第２の内部認証に成功すれば，ステップＳ２１０８においてダウンロードが許可されるが，第２の内部認証に失敗すれば，コンテンツの情報配信（ＤＬ）動作は拒絶される（ステップＳ２１１２）。

【０１７９】（４．３　ダウンロード動作）以上のようにして，図２０に示すステップＳ２１０６において内部認証が完了した後に，ステップＳ２２０６において，メモリスティックなどの所定の記憶媒体にコンテンツをダウンロードする。

【０１８０】以下，図２２を参照しながら，内部認証，復号化処理，ダウンロード処理の連携関係について詳細に説明する。

【０１８１】まずデバイス鍵（ＫｄｅｖｉｃｅＡ）をセキュアに保持する情報提供装置４２０は，ダウンロード対象のパッケージのＭＡＣ値をチェックして，ダウンロード対象のパッケージが正規のオーサリングシステムにより作成されたものであり改ざん等がされていないことを確認する。

【０１８２】情報提供装置４２０は，パッケージに含まれるコンテンツ使用可能化鍵（ＥＫＢ）をデバイス鍵

（ＫｄｅｖｉｃｅＡ）で復号してルート鍵（ＫｒｏｏｔＡ）を取得する。情報提供装置４２０は，コンテンツ使用可能化鍵（ＥＫＢ）をリーダ／ライタ４３０に送信する。リーダ／ライタ４３０も，情報提供装置４２０と同様に，デバイス鍵（ＫｄｅｖｉｃｅＢ）をセキュアに保持している。リーダ／ライタ４３０は，情報提供装置４２０から受け取ったコンテンツ使用可能化鍵（ＥＫＢ）をデバイス鍵（ＫｄｅｖｉｃｅＢ）で復号化して，ルート鍵（ＫｒｏｏｔＢ）を取得する。

【０１８３】情報提供装置４２０とリーダ／ライタ４３０は，双方のルート鍵（ＫｒｏｏｔＡ，ＫｒｏｏｔＢ）を比較し，第２の内部認証を行う。

【０１８４】内部認証に成功すると，さらにコンテンツの正当性をチェックしてから，リーダ／ライタ４３０により，メモリスティックなどの記憶媒体にコンテンツをコピーする。

【０１８５】この段階では，コンテンツはまだコンテンツ鍵（Ｋｃ）により暗号化されており，再生は不可能である。そこで，コンテンツ鍵（Ｋｃ）を用いて，コピーしたコンテンツを再生制御装置により再生可能状態にすることにより，ユーザは，自己所有の再生装置１８４によりコンテンツを楽しむことが可能となる。

【０１８６】（４．４　複数コンテンツの一括ダウンロード動作）図２２に示す例では，一つのコンテンツをコピーする例を示したが，本実施の形態にかかる情報配布システムにおいては，複数のコンテンツを同時にダウンロードすることも可能である。

【０１８７】図２３を参照しながら，複数コンテンツの一括ダウンロード動作について説明する。所定の認証動作が成功した後に，情報提供装置４２０は，リーダ／ライタ４３０を介して，所定の記憶媒体１８２に対して，第１のパッケージをコピーする。この段階では，第１のパッケージにかかるコンテンツの再生は不可能である。次いで，情報提供装置４２０は，リーダ／ライタ４３０を介して，所定の記憶媒体１８２に対して，第２および第３のパッケージをコピーする。このようにして，複数のコンテンツの一括ダウンロードが完了すると，再生制御装置は，ダウンロードが完了した複数のコンテンツをまとめて再生可能状態にする。

【０１８８】このように，ダウンロードする度に１曲１曲再生可能にするのではなく，例えば３曲のダウンロード要求に対して３曲書き込んだ後に３曲分一括に再生可能にすることにより，複数のコンテンツを一括ダウンロードする際の認証等の手間を大幅に軽減することができる。

【０１８９】（４．５　ダウンロード後のコンテンツの流れ）次に図２４を参照しながら，本実施の形態にかかる情報配信システムによりダウンロードしたコンテンツのその後の流れについて説明する。

【０１９０】図２４に示すように，本システムによれば，キオスク端末（情報配信装置）４００から一旦メモリスティックのような記憶媒体にパッケージ化されたコンテンツはダウンロードされる。パッケージ内には，コンテンツの利用条件に関する情報も含まれており，この条件に従って，ダウンロード後のコンテンツの処理方法が決定される。

【０１９１】通常は，メモリスティックなどの記憶媒体１８２からパーソナルコンピュータなどの端末装置１９０にコンテンツをインポートする。そして，端末装置１９０から再び再生機能を有する携帯機器１９２，１９４，１９６にコンテンツをチェックアウトすることが可能である。チェックアウトの回数は，著作権保護のために，制限されており，図示の例では，３回のチェックアウトが許可されている。したがって，３種類の携帯機器１９２，１９４，１９６に対してダウンロードしたコンテンツをコピーすることが可能である。

【０１９２】チェックアウト回数を超えて，上記携帯機器１９２，１９４，１９６以外の再生装置にコンテンツをコピーしたい場合には，いずれかの携帯機器１９２，１９４，１９６から一旦コンテンツをパーソナルコンピュータ１９０にチェックインした後に，許可されたチェックアウトの回数内でコピーすることが可能となる。

【０１９３】以上説明したように，本実施の形態にかかる情報配信システムによれば，オーサリング時点でコンテンツを暗号化しているので，情報配信端末側でのダウンロード時間を短縮し，情報配信端末側の負荷を軽減することができる。

【０１９４】本実施の形態にかかる情報配信システムによれば，情報配信端末側では，正規のオーサリング装置で作成したコンテンツしかダウンロードできないように制限をかけているので，オーサリング後に中身を一部手で書き換えるといったような不正行為を防止できる。また不正にオーサリングしたコンテンツを情報配信端末に持ってきてもそのコンテンツをダウンロードすることができない。

【０１９５】本実施の形態にかかる情報配信システムによれば，正規のコンテンツであっても，単純に記憶媒体にコピーしただけでは再生可能にはならない。再生可能にするには，情報提供装置側において外部認証および内部認証が必要となるため，不正コピーを防止できる。

【０１９６】本実施の形態にかかる情報配信システムによれば，正規購入したコンテンツファイルは何回でもダウンロード可能であり，また正規にダウンロードしたコンテンツファイルをＰＣに移動させ，ＰＣと他の装置との間でチェックアウト／チェックインすることができる。

【０１９７】本実施の形態にかかる情報配信システムによれば，楽曲ファイルなどのメインコンテンツ以外にも，ジャケット写真等の付随データもメインコンテンツに関連付けて処理することができる。

【０１９８】以上，添付図面を参照しながら本発明にかかる情報配信システム等の好適な実施形態について説明したが本発明はかかる例に限定されないことは言うまでもない。当業者であれば，特許請求の範囲に記載された技術的思想の範疇内において，各種の変更例または修正例に想到し得ることは明らかであるが，それらについても当然に本発明の技術的範囲に属するものと了解される。

【０１９９】例えば，上記実施形態においては，本発明にかかる情報配信システム等の好適な実施形態として，当該システムを音楽データを配信用コンテンツとして配信するシステムに適用した場合について説明したが，本発明はかかる例に限定されない。例えば，当該システムは，音楽データ以外にも，画像（静止画および動画を含む）データ，ゲームプログラムなどの様々なコンテンツデータをネットワークを介してユーザに対して配信する情報配信システムにも適用可能であることはいうまでもない。

【０２００】

【発明の効果】以上説明したように，本発明によれば，不正なコピーを有効に防止して楽曲データなどの配信することが可能な情報配信システムを構築できる。すなわち，本発明によれば，オーサリング時の不正操作，配信時の不正操作，情報配信端末の不正操作，ダウンロード時の不正操作を有効に防止することが可能である。さらに，本発明によれば，オーサリング時に圧縮および暗号化を行うので，ダウンロードに時間がかからない情報配信システムを構築することが可能である。

【図面の簡単な説明】

【図１】本発明の実施の一形態にかかる情報配信システム１００の概略構成を示すブロック図である。

【図２】本発明の実施の一形態にかかる情報配信システム１００のコンテンツホルダ１２０の概略構成を示すブロック図である。

【図３】本発明の実施の一形態にかかる情報配信システム１００のコンテンツアグリゲータ２００の概略構成を示すブロック図である。

【図４】本発明の実施の一形態にかかる情報配信システム１００のオーサリングスタジオ３００の概略構成を示すブロック図である。

【図５】本発明の実施の一形態にかかる情報配信システム１００におけるオーサリングスタジオ３００ののオーサリング部３１０の概略構成を示すブロック図である。

【図６】本発明の実施の一形態にかかる情報配信システム１００のオーサリングシステムにおけるオーサリング装置３１６とオーサリング鍵生成装置１６０との関係の概略構成を示すブロック図である。

【図７】本発明の実施の一形態にかかる情報配信システム１００のオーサリングシステムの構築例を示すブロック図である。

【図８】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００の概略構成を示すブロック図である。

【図９】本発明の実施の一形態にかかる情報配信システム１００の情報提供部４２０の概略構成を示すブロック図である。

【図１０】本発明の実施の一形態にかかる情報配信システム１００の情報提供部４２０の外部認証部４２２の概略構成を示すブロック図である。

【図１１】本発明の実施の一形態にかかる情報配信システム１００の情報提供部４２０の内部認証部４２４概略構成を示すブロック図である。

【図１２】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００のシステム構成例を示すブロック図である。

【図１３】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００において行われる外部認証（ローカル）の一例を示すブロック図である。

【図１４】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００において行われる外部認証（リモート）の一例を示すブロック図である。

【図１５】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００において行われる外部認証（セミローカル）の一例を示すブロック図である。

【図１６】本発明の実施の一形態にかかる情報配信システム１００のオーサリング鍵生成工程を示すフローチャートである。

【図１７】本発明の実施の一形態にかかる情報配信システム１００のオーサリング鍵生成工程を示す説明図である。

【図１８】本発明の実施の一形態にかかる情報配信システム１００のオーサリング工程を示すフローチャートである。

【図１９】本発明の実施の一形態にかかる情報配信システム１００の配信対象である暗号化コンテンツ（Ｅ（Ｋｃ，Ｃｏｎｔｅｎｔ）），ルート鍵で暗号化されたコンテンツ鍵（ＥＫｃ）およびコンテンツ使用可能化鍵（ＥＫＢ）の構成を示す説明図である。

【図２０】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００における情報配信工程を示すフローチャートである。

【図２１】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００におけるコンテンツ復号工程を示すフローチャートである。

【図２２】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００におけるパッケージのダウンロード工程を示すフローチャートである。

【図２３】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００における複数のパッケージを一括してダウンロードするダウンロード工程を示

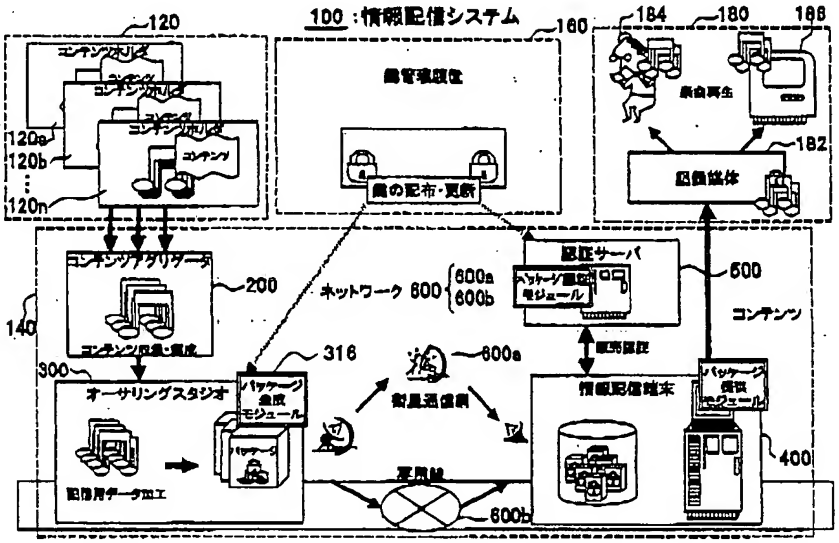
すフローチャートである。

【図２４】本発明の実施の一形態にかかる情報配信システム１００の情報配信端末４００において一旦ダウンロードしたコンテンツのその後の処理について示す説明図である。

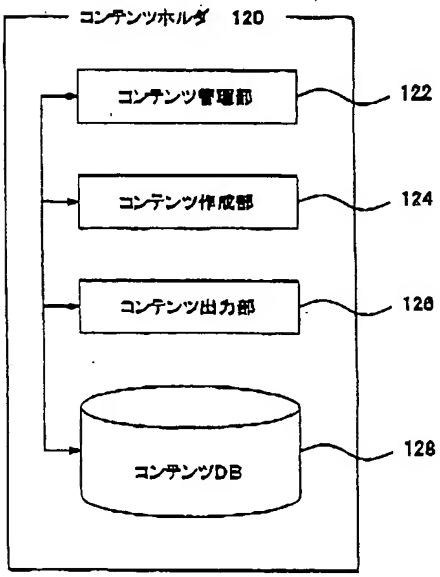
【符号の説明】

１００　情報配信システム
１２０　コンテンツホルダ
１４０　コンテンツ流通部
１６０　鍵管理装置（オーサリング鍵生成装置）
１８０　ユーザ
２００　コンテンツアグリゲータ
３００　オーサリングスタジオ
４００　情報配信端末（キオスク端末）
５００　認証サーバ
６００　ネットワーク

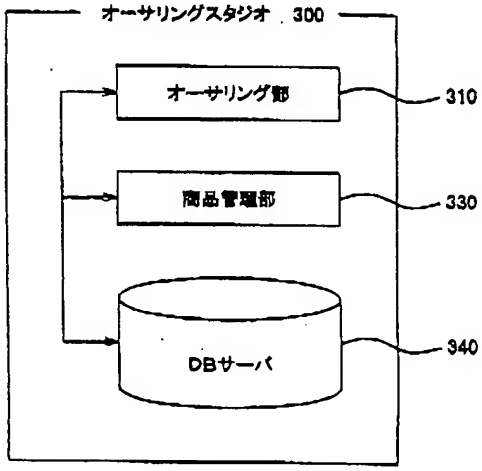
【図１】



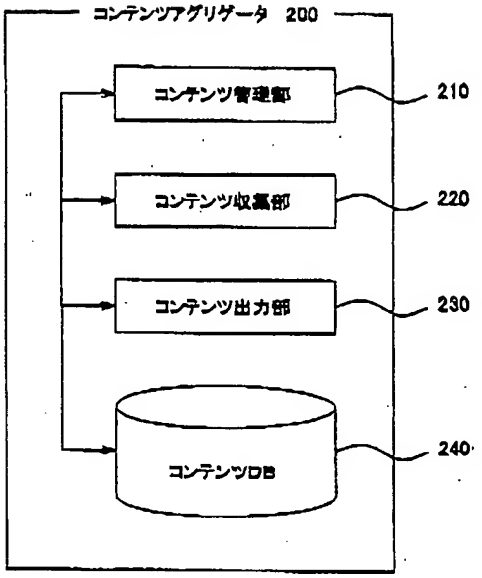
【図２】



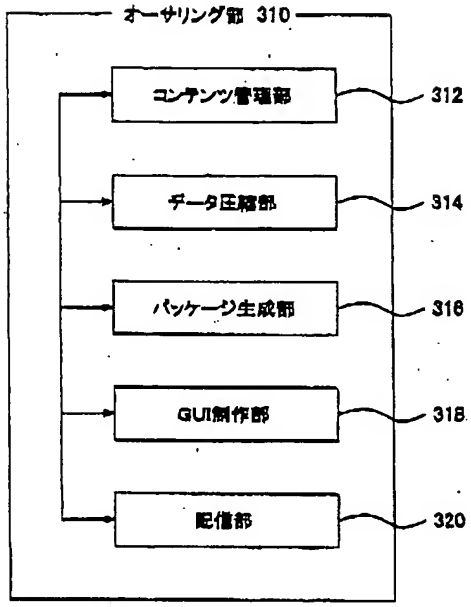
【図４】



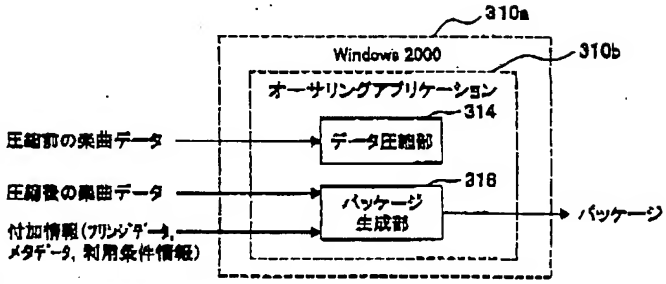
【図３】



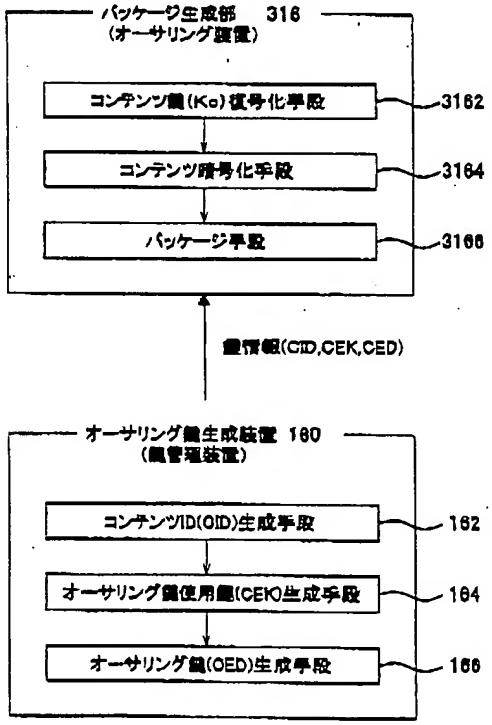
【図５】



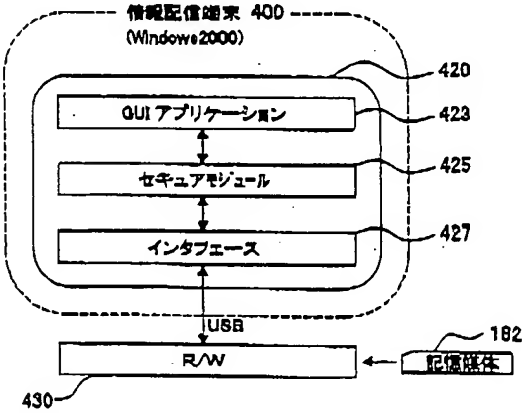
【図７】



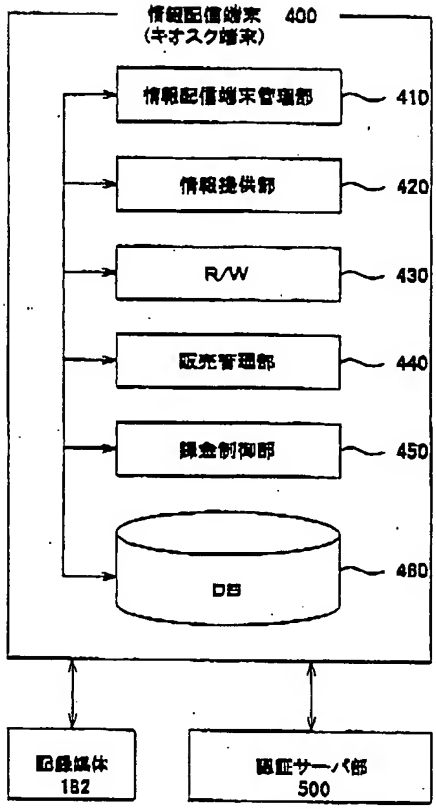
【図６】



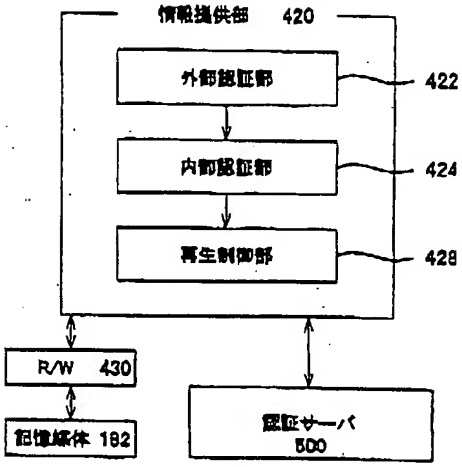
【図１２】



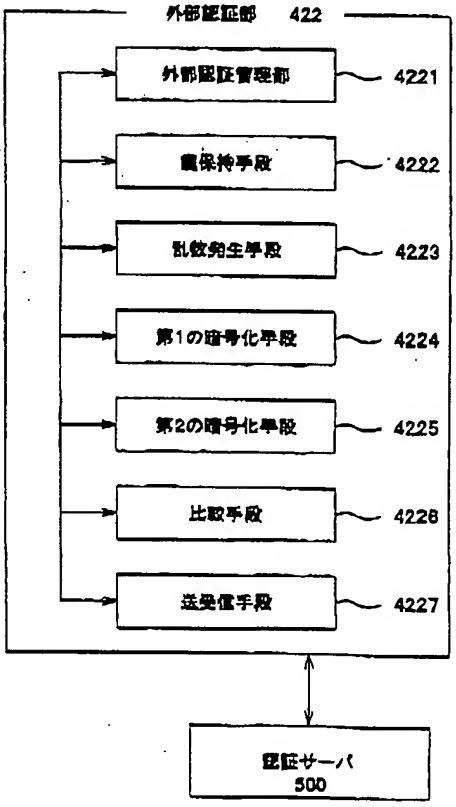
【図８】


情報配信端末 400
(キオスク端末)
情報配信端末管理部
410
情報提供部
420
R/W
430
販売管理部
440
課金制御部
450
DB
460
記録媒体
182
認証サーバ部
500

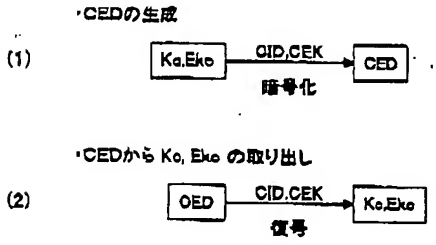
【図９】


情報提供部 420
外部認証部
422
内部認証部
424
再生制御部
428
R/W 430
記憶媒体 182
認証サーバ
500

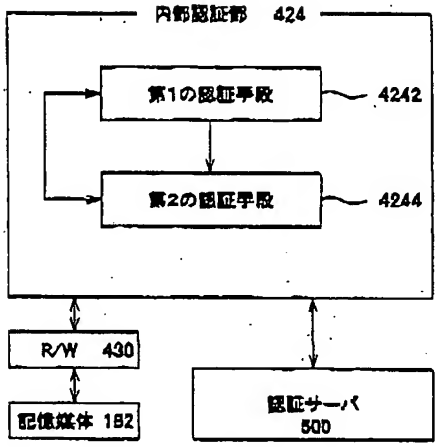
【図１０】


外部認証部 422
外部認証管理部
4221
鍵保持手段
4222
乱数発生手段
4223
第1の暗号化手段
4224
第2の暗号化手段
4225
比較手段
4226
送受信手段
4227
認証サーバ
500

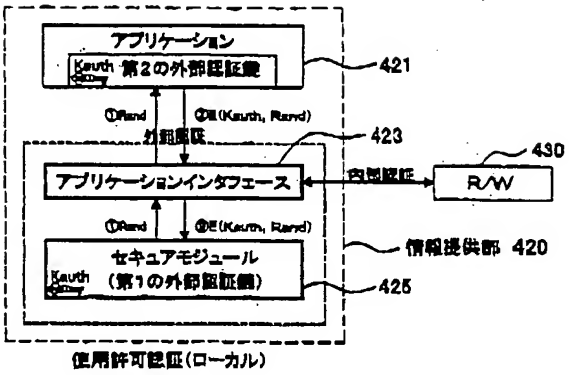
【図１７】


・CEDの生成
(1)
Ko,Eko
CID,CEK
暗号化
CED
・CEDから Ko, Eko の取り出し
(2)
CED
CID,CEK
復号
Ko,Eko

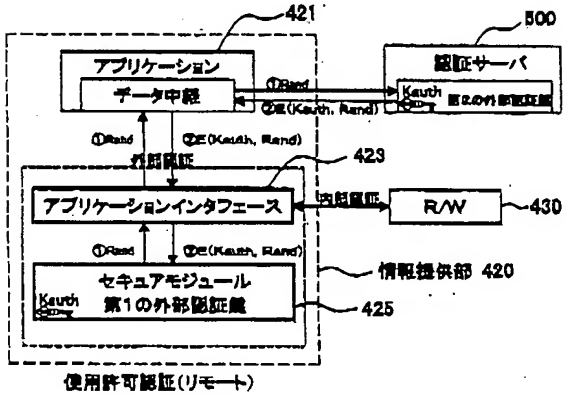
【図１１】



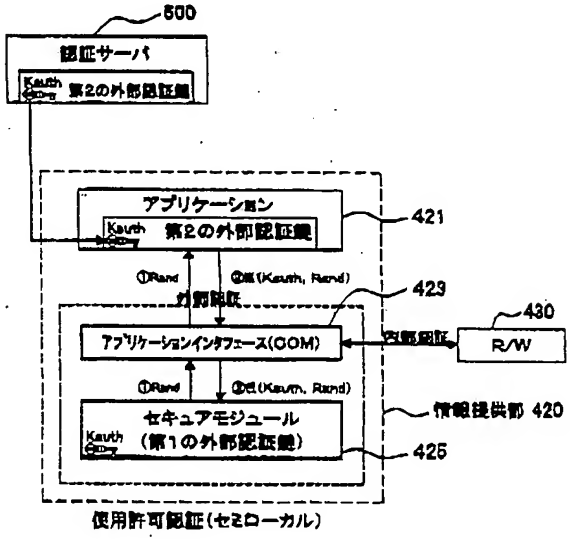
【図１３】



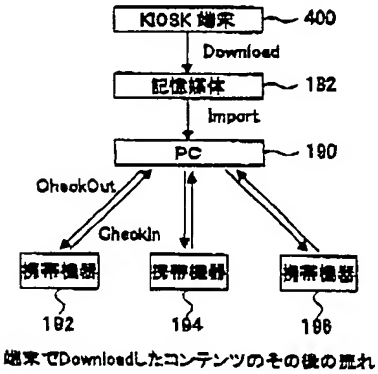
【図１４】



【図１５】

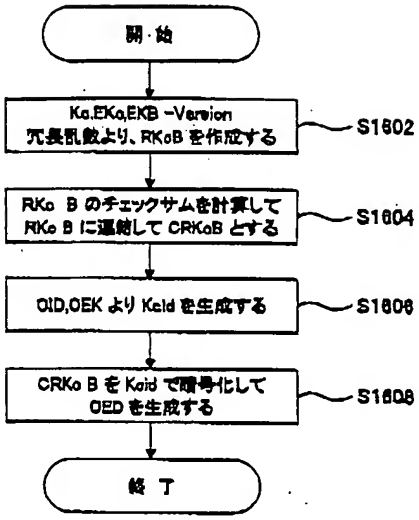


【図２４】



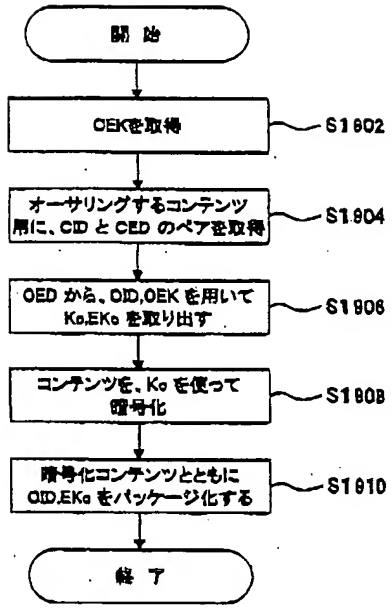
端末でDownloadしたコンテンツのその後の流れ

【図１６】



OED作成フロー

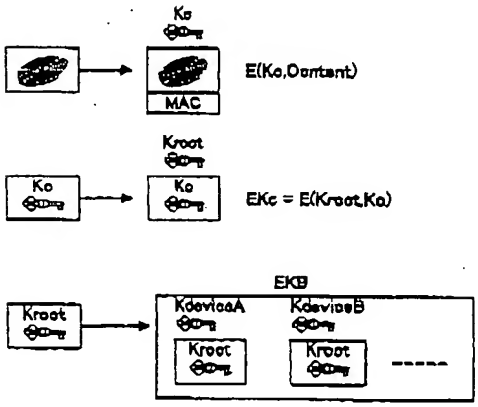
【図１８】



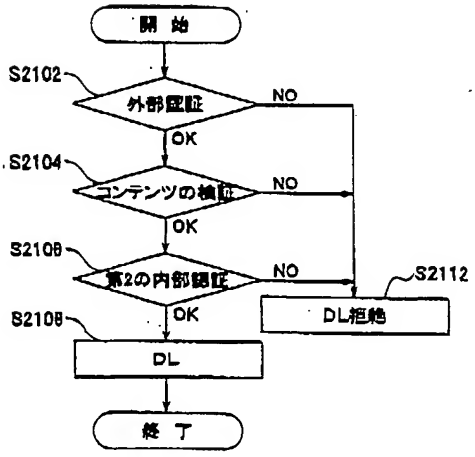
オーサリングフロー

【図１９】

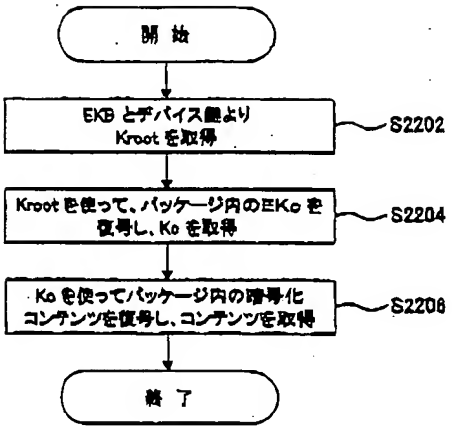
コンテンツの暗号化、Eko の生成、EKB の生成



【図２０】

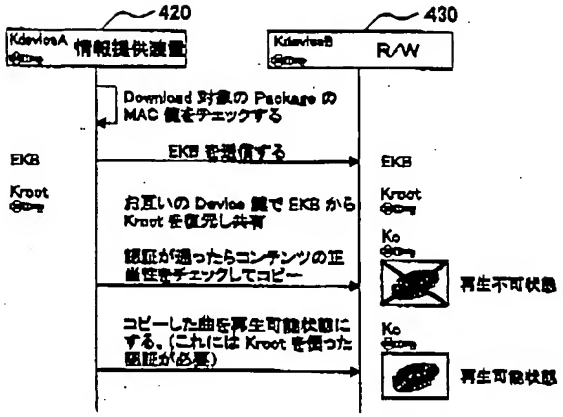


【図２１】



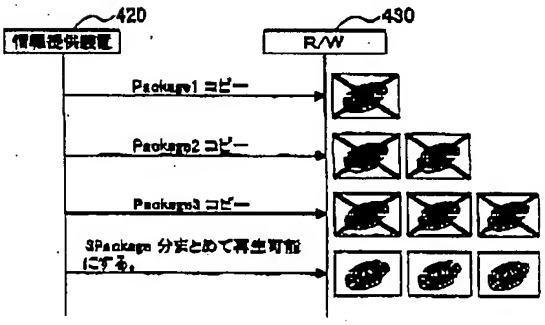
コンテンツ復号フロー

【図２２】



パッケージのダウンロードの流れ

【図２３】



複数パッケージのダウンロード

フロントページの続き

(72)発明者 上野 信一
東京都品川区北品川６丁目７番35号 ソニー株式会社内

Ｆターム(参考) 5B085 AA08 AE29
5J104 AA01 AA13 AA16 EA04 EA26 NA02

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☑ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.